SOUTH WEST UNIVERSITY
"NEOFIT RILSKI"

Мария Христос Бици

АВТОРЕФЕРАТ
на
ДОКТОРСКА ДИСЕРТАЦИЯ

на тема

ОСИГУРЯВАНЕ НА ЗАЩИТА НА КОМПЮТЪРНА И МРЕЖОВА ИНФОРМАЦИЯ В ГРЪЦКАТА ПУБЛИЧНА АДМИНИСТРАЦИЯ ЧРЕЗ ИЗПОЛЗВАНЕ НА ТЕХНОЛОГИИ „STATE-OF-THE-ART"

Ръководител: Проф. д-р Нина Синягина

БЛАГОЕВГРАД 2026

БЛАГОДАРНОСТИ

Преди да представя тази докторска дисертация, считам за необходимо да се спра на онези специални хора, с които имах щастието да работя през цялото това време. Благодаря на всички от сърце! По-специално, бих желала да благодаря на ръководителя професор доктор Нина Синягина, за нейния съществен принос, за научните насоки и съвети, както и за материалната и морална подкрепа, които получих от нея, на всички етапи от изпълнението на този изследователски проект.

Също така, приносът на моите професори Стефан Стефанов и Петрана Стойкова беше решаващ, на които трябва да изразя искрената си благодарност за големия им принос за завършването на обучението ми.

Същевременно искам горещо да благодаря на членовете, на научното жури, които посветиха значителна част от ценното си време за проучване и оценка на работата по тази дисертация.

След това, благодаря на моята приятелка Антула за цялостната подкрепа. На децата си Димитрис, Кристина - Лемония, Зоуи - Смарагда, Рафаел - Фотини, Зинаида - Роксана и Мириам - Клео, за тяхното търпение и разбиране, За времето и вниманието, от което ги лиших по време на докторската си дисертация. В заключение, благодаря на моя съпруг Вангелис, за помощта, разбирането и доверието, които ми оказваше през всичките тези години, за вярата му в мен и възможностите ми, за подкрепата му във всяко мое начинание.

СЪДЪРЖАНИЕ

ПРЕДГОВОР

Дигиталните технологии са неразделна част от ежедневието и оказват огромно влияние върху публичната администрация и обществените услуги, променяйки начина, по който се осъществява дейността на администрацията и ежедневните услуги, предлагани на гражданите и частната икономика.

В световен мащаб, публичните администрации на държавите се опитват да прекроят административните структури по такъв начин, че да ги направят по-ефективни, по-бързи и с по-ниски разходи. Това начинание изисква усилия за промяна, като въвеждане на Нова публична администрация, реформа, която се стреми да разреши проблемите на старата публичната администрация, чрез прилагане на идеи и практики, произтичащи от частния сектор.

Част от тази реформа е въвеждането на Електронноправителство. Това е философия на промяната на обществените услуги, чрез въвеждане и използване на инструментите, предлагани от технологиите. Електронното правителство всъщност еизползването на технологии от публичната администрация за изпълнение на нейните дейности,за комуникацията и ежедневните транзакции с гражданите и организациите.

В настоящото изследване интересът е насочен къмтеми свързани с подобряването на сигурността наинформационните системи на гръцкия публичен сектор, с използването на най-съвременни технологии. Използването на информационни системи в публичния сектор е наложително и днес няма публична организация, която да се стреми къмразвитие, без да инвестира в нови технологии,

без да се опитва да подобри позициите си на вътрешния и световния пазар.
Cloud computing е иновативна технология, която позволява на организациите да подобрят бизнеса си, да обслужват клиентите си по-бързо, да намалят разходите и да станат по-конкурентоспособни.

КЛЮЧОВИ ДУМИ:
Информационни системи, информационни системи за управление, сигурност на информационните системи и мрежи, електронно управление, публична администрация, съвременни технологии, облачни изчисления.

ГЛАВА 1: ИНФОРМАЦИОННИ СИСТЕМИ

Повече от всякога организациите по света разглеждат информацията като един от своите най-ценни ресурси. Поради тази причина не е изненадващо, че информационните системи представляват основен градивен елемент на съвременните организации и се използват за подпомагане на всички видове организационни функции и дейности.

В научната литература съществуват множество определения на понятието „информационна система“, които се различават в по-голяма или по-малка степен помежду си. В рамките на настоящата дисертация информационната система се определя като оперативна система, която обработва данни от външната и вътрешната среда на организацията и предоставя информация на нейното ръководство, така че да могат да бъдат вземани бързи, правилни и обосновани решения.

За целите на настоящото изследване е избрано по-подробно представяне на информационните системи от стратегическо ниво, тъй като към тях принадлежат и информационните системи на публичната администрация, които са предмет на настоящата дисертация.

По-конкретно:

1. Системи за обработка на транзакции (Transaction Processing Systems – TPS)

В организациите събирането и поддържането на записи за ежедневните транзакции са сред първите процеси, които започват да се извършват чрез използването на компютърни технологии. Чрез тези системи се автоматизират повтарящите се дейности и операции.
Системите за обработка на транзакции предоставят на оперативното ръководство информация, свързана с основните дейности и ежедневните операции на организацията. Те представляват компютъризирани системи, които изпълняват и регистрират текущи рутинни транзакции, необходими за осъществяването на организационната дейност.

2. Управленски информационни системи (Management Information Systems – MIS)

Мениджърите на средно управленско ниво се нуждаят от системи, които да подпомагат наблюдението, контрола и вземането на решения в управленската дейност.
Управленските информационни системи предоставят на средното управленско ниво отчети за текущото състояние и представяне на организацията. Тази информация се използва за наблюдение и контрол на дейността, както и за прогнозиране на бъдещите резултати.
Като цяло MIS предоставят отговори на рутинни въпроси, които са предварително идентифицирани и за които съществуват установени процедури за обработка. Те подпомагат управленските решения

чрез генериране на справки и анализи, ориентирани към по-дългосрочни цели, за разлика от TPS, които се фокусират върху ежедневните операции и рутинните процеси (Osterle, 2013).

3. Системи за подпомагане на вземането на решения (Decision Support Systems – DSS)

Системите за подпомагане на вземането на решения подпомагат предимно мениджърите от средно ниво при решаването на нерутинни проблеми.
Тези системи комбинират данни, аналитични модели и удобен за потребителя софтуер в единна интегрирана система, способна да подпомага решаването на полуструктурирани или неструктурирани проблеми.
Те са насочени към уникални и бързо променящи се ситуации, при които процесът на вземане на решение не може да бъде напълно определен предварително. За разлика от MIS, които обработват предимно рутинни и предварително планирани решения, DSS подпомагат проблеми, които изискват активната намеса и професионалната преценка на ръководителя.
Освен това DSS не разчитат единствено на вътрешна информация от TPS, както обикновено правят MIS, а са проектирани така, че да интегрират и външни източници на информация в аналитичния процес (DaSilva & Reikman, 2014).
Системите DSS са разработени така, че потребителите да могат да взаимодействат директно с тях чрез специализиран и удобен интерфейс. В много случаи тези системи се определят и като системи за бизнес интелигентност (Business

Intelligence Systems), тъй като тяхната основна цел е подпомагането на по-качествени управленски решения (Laudon & Laudon, 2009, pp. 55–57).

4. Системи за подпомагане на висшето ръководство (Executive Support Systems – ESS)

Системите за подпомагане на висшето ръководство представляват информационни системи, предназначени да подпомагат висшите мениджъри при получаването, обработката и използването на информацията, необходима за поддържане на цялостната ефективност на организацията.
Тези системи са насочени основно към предоставяне на информация за стратегическо управление и вземане на стратегически решения. Те подпомагат висшето ръководство при адаптирането към промените във външната среда, като отчитат силните и слабите страни на организацията.
ESS са предназначени за работа с неструктурирани проблеми, които изискват преценка, анализ и интуиция, тъй като не съществува предварително установена процедура за тяхното решаване.
Тези системи интегрират информация както от външната среда, така и от вътрешните MIS и DSS системи. Те филтрират, обобщават и наблюдават критични данни, като представят на висшето ръководство единствено информацията с най-висока стратегическа стойност.

5. Експертни системи (Expert Systems – ES)

Експертните системи представляват специализиран вид информационни системи, базирани на човешки експертни знания в конкретна област.
Те се разработват въз основа на знанията и опита на специалисти с цел решаване на проблеми, които обикновено изискват човешка експертиза. По същество те имитират начина, по който ръководителите и експертите вземат решения в сложни и неструктурирани ситуации.
За да предоставят решение на проблеми, при които информацията често е непълна, неясна или несигурна, експертните системи използват евристични методи за намиране на удовлетворително решение, което не винаги е оптималното, но е практически приложимо (Eikonomou & Georgopoulos, 1995, p. 95).
Стратегическите информационни системи, разгледани по-горе, са взаимозависими. Системите за обработка на транзакции обикновено представляват основния източник на данни за останалите системи, докато системите за подпомагане на висшето ръководство са основните получатели на информация от по-ниските организационни нива. Същевременно между различните видове системи съществува постоянен обмен на данни и информация.
В заключение, всяка организация, чрез анализ на своята вътрешна и външна среда и чрез идентифициране на силните и слабите си страни, както и на възможностите и заплахите, формира своята стратегия. След формулирането на стратегията следва нейното прилагане, а

впоследствие и оценка и контрол на постигнатите резултати, с цел установяване на евентуални отклонения от желаните резултати и предприемане на необходимите коригиращи действия.

В този процес информационните системи играят особено важна роля. Следователно конкурентното предимство на организацията не произтича единствено от използването на ERP система, а от правилния избор и успешното ѝ внедряване (Sfyris, 2017).

Информационните системи, в съчетание със съвременните технологии, могат да направят една организация по-ефективна, по-резултатна и по-иновативна при предоставянето на услуги. За да бъдат реализирани тези ползи, е необходимо новите технологии и информационните системи да бъдат внедрявани в съответствие със стратегическите цели на организацията.

Днес технологиите представляват основа за развитието на всяка организация. Те непрекъснато се развиват и особено в сферата на обслужването на гражданите са абсолютно необходими, тъй като улесняват комуникацията между публичната администрация и гражданите, подобряват вътрешните процеси и повишават скоростта на обслужване. Непрекъснатата модернизация е жизненоважна предпоставка за бъдещото развитие на организациите и институциите.

СИГУРНОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

Проблемът със сигурността на информационните системи е особено актуален в съвременната епоха. Непрекъснато нарастващото използване на технологии, базирани на бази данни и комуникационни мрежи, както и значимата роля на информационните системи за функционирането на организациите, правят необходима реализацията на мерки за защита на информацията и информационните ресурси.
Понятието „сигурност на информационните системи“ е свързано със способността на една организация да защитава своята информация от изменения, унищожаване и неоторизирано използване на ресурсите си.
Сигурността на информационните системи включва три основни измерения:

а) Превенция, която включва мерки за предотвратяване на възможни щети върху компонентите на информационната система;

б) Откриване, което включва установяване кога, как и от кого е причинена повреда или нарушение в компонентите на информационната система;

в) Реакция, която включва възстановяване или реконструкция на засегнатите компоненти на информационната система.

Концепцията за сигурност е тясно свързана с три основни принципа:

- Конфиденциалност (Confidentiality);
- Цялостност (Integrity);
- Наличност (Availability).

Освен тях съществено значение имат и следните характеристики:

- Оторизирано използване на системата от упълномощени потребители;
- Автентичност на съобщенията;
- Неотричане на извършените действия (Non-repudiation);
- Отчетност (Accountability);
- Надеждност и безопасност на системите.

Въпреки това всяка информационна система е изложена на различни уязвимости. Под уязвимост се разбира слабост или недостатък в системата за сигурност, който може да бъде използван от нападател.

Основните категории уязвимости включват:

- физически уязвимости;
- природни уязвимости;
- хардуерни и софтуерни уязвимости;
- комуникационни уязвимости;
- човешки уязвимости.

Заплаха за информационната система представлява всяка ситуация, която може да причини щети или загуби, като злонамерени действия на хора, човешки грешки, природни бедствия или вътрешни дефекти в оборудването и софтуера.

Основните видове заплахи по отношение на хардуера, софтуера и данните са:

- прихващане (interception);
- модификация (modification);
- подправяне (fabrication);
- прекъсване (interruption).

За ограничаване на уязвимостите и заплахите е необходимо да бъдат внедрени подходящи защитни мерки.
Защитните мерки представляват процедури, техники, действия и средства, които ограничават уязвимостите на информационната система.

Те обхващат следните основни области:

- физическа сигурност;
- сигурност на компютърните системи;
- сигурност на базите данни;
- мрежова сигурност.

Сред най-разпространените средства за защита се открояват:

Криптография

Криптографията (шифроването) представлява процес на кодиране на информацията и е една от най-широко използваните технологии за защита на електронните комуникации в незащитени мрежови среди (Wallace, 2014).

Софтуерни средства за защита

Те включват антивирусни системи, защитни стени, системи за откриване на проникванията и други специализирани решения за защита на информационните активи.

Хардуерни средства за защита

Включват специализирани устройства и инфраструктури, предназначени да осигурят сигурността на информационните системи.

Политики за сигурност

Политиките за сигурност определят правилата, процедурите и механизмите за управление на сигурността в организацията (Pangalos & Mavridis, 2002).
Тъй като хората често поставят производителността над сигурността, те могат да пренебрегнат мерките за защита, ако ги възприемат като пречка за изпълнение на задачите си.
Социалното инженерство използва именно тези човешки слабости с цел манипулиране на потребителите и придобиване на чувствителна информация или заобикаляне на защитните механизми.
Обучението и повишаването на информираността относно връзката между сигурността, етиката и защитата на личните данни представляват важни инструменти за ограничаване на подобни рискове (Wallace, 2014).

В заключение може да се отбележи, че информационните системи са от съществено значение за развитието и функционирането на публичните услуги. Представените системи на стратегическо ниво включват и тези, използвани в публичната администрация, които са предмет на настоящото изследване.

Използването им в публичния сектор е задължително условие за модернизацията и развитието на институциите. Днес не съществува публична организация, която да се стреми към развитие, без да инвестира в нови технологии и без да използва информационни системи за подобряване на своето функциониране и конкурентоспособност.

Гръцката държава, която дълги години функционираше въз основа на традиционен бюрократичен модел, е изправена пред необходимостта от дълбока трансформация чрез внедряване на нови технологии и съвременни управленски модели.

Особено в периоди на икономически затруднения технологиите могат да допринесат за намаляване на разходите и едновременно с това за повишаване качеството на предоставяните услуги.

Следващата глава разглежда по-задълбочено въпросите, свързани със сигурността на информационните системи.

ГЛАВА 2. СИГУРНОСТ НА ИНФОРМАЦИОННИТЕ СИСТЕМИ

През последните години се наблюдава изключително бързо развитие на информационните системи. Голям брой организации от публичния и частния сектор разчитат на тяхното функциониране за осъществяване на ежедневната си дейност. Чрез тези системи се обменя информация, предоставят се услуги и се обработват огромни обеми от данни.

Сигурността на информационните системи представлява критичен фактор за ефективното функциониране и устойчивостта на всяка организация. Дори минимално нарушение, прекъсване или неоторизиран достъп до информационните системи може да доведе до значителни финансови загуби, нарушаване на работните процеси и дори до невъзможност за нормалното функциониране на организацията.

Особено сериозни са рисковете за системите, в които се съхраняват чувствителни данни, поверителна информация и критични административни функции. Поради тази причина е необходимо внедряването на подходящи механизми за защита срещу разнообразните заплахи, на които тези системи могат да бъдат изложени.

Проблемът със сигурността на информационните системи съществува още от самото начало на развитието на информационните технологии. В

съвременната цифрова среда обаче рискът е значително по-голям, тъй като системите са достъпни за широк кръг потребители и са изложени на разнообразни външни и вътрешни заплахи.
Независимо от формата, в която съществува информацията, когато тя има стойност за организацията, трябва да бъде правилно съхранявана и надеждно защитена. Основната цел на информационната сигурност е защитата на информацията от широк спектър от заплахи, които могат да компрометират нейната конфиденциалност, цялостност и наличност.
Може да се приеме, че ако сигурността бъде представена под формата на пирамида, нейната основа безспорно е разработването и внедряването на цялостна политика за сигурност. Политиката за сигурност представлява основният инструмент за управление на сигурността на информационните системи, въпреки че съдържанието и значението на понятието могат да варират в зависимост от целите, средата и организационния контекст, в който се прилага (Karyda, 2005).
Разработването на политики за сигурност е пряко свързано както с техническите процедури, така и с административните мерки, които се прилагат за защита на информационните системи срещу случайни или умишлени заплахи.
Най-важният етап при създаването на една политика за сигурност е идентифицирането на информационните активи, които трябва да бъдат защитени, както и извършването на анализ и оценка на риска.
Политиката за сигурност трябва да предоставя ясни отговори на следните въпроси:

- Каква е основната цел на политиката?
- Кои информационни активи се нуждаят от защита?
- Кой носи отговорност за тяхната защита и какви са неговите задължения?

Сигурността на информационните системи се основава на три фундаментални принципа:

- Цялостност (Integrity);
- Наличност (Availability);
- Конфиденциалност (Confidentiality).

Управлението на сигурността не е лесна задача, но е задължително условие за ефективното функциониране на съвременните организации. Внедряването на информационни системи води до повишаване на производителността и ефективността, но същевременно създава нови рискове, които трябва да бъдат идентифицирани и управлявани по подходящ начин (Elky, 2006).
За щастие индустрията за информационна сигурност предлага широк набор от инструменти, методологии, контроли и политики, предназначени за справяне със заплахите. Въпреки това интегрирането на всички тези механизми във всяка организация е сложен процес.
Различните организационни структури, бизнес процеси и нива на ресурсно осигуряване създават уникални условия за всяка организация. Поради това мерките за сигурност трябва да бъдат адаптирани към конкретните особености на всяка среда, така че сигурността да подпомага организационната дейност,

а не да се превръща в пречка за нейното развитие (Karnavas, 2012).
Един от най-важните инструменти за управление на сигурността е анализът на риска.
Анализът на риска има за цел:

- да идентифицира активите на организацията;
- да открие съществуващите уязвимости;
- да определи потенциалните заплахи;
- да оцени възможните последствия от реализирането на даден риск.

Под понятието „активи“ не следва да се разбират единствено финансови ресурси. Към тях се отнасят и личните данни, организационната репутация, критичната информация и всички ресурси, чието компрометиране може да доведе до сериозни последици за организацията.
Чрез анализа на риска може да бъде определено кои контрамерки са икономически оправдани и в кои случаи е приемливо определен риск да бъде поет от организацията.
Освен това анализът на риска позволява приоритизирането на мерките за защита, което е особено важно в условията на ограничени финансови ресурси.
В съвременната икономическа среда, характеризираща се с ограничения в бюджетите на организациите, анализът на риска придобива още по-голямо значение, тъй като позволява оптимално разпределение на ресурсите за сигурност.
Основната цел на системата за управление на сигурността е ограничаването на риска до приемливо ниво.

Тази система включва:

- оценка на риска;
- определяне на приемливото ниво на риск;
- разработване на политика за сигурност;
- внедряване на мерки за защита;
- създаване на организационна рамка за управление на сигурността;
- осигуряване на необходимите човешки и финансови ресурси.

Политиката за сигурност, съчетана с техническите и организационните мерки за защита, формира цялостния план за сигурност на информационните системи на организацията.
Изборът на методология за анализ и управление на риска зависи от редица фактори, сред които:

- размерът и сложността на информационната система;
- разходите за внедряване;
- организационната култура;
- наличието на специализиран софтуер;
- опитът и подготовката на специалистите;
- степента на покриване на техническите и социалните аспекти на сигурността (Kokolakis, 2000).

Особено важна роля в процеса има служителят по информационна сигурност, който трябва да притежава необходимите знания и компетенции и да бъде официално упълномощен от ръководството да изпълнява тази функция.

Голямото разнообразие от средства за атака и непрекъснатото развитие на нови техники за проникване представляват сериозно предизвикателство за сигурността на информационните системи.
Историята многократно е доказала, че не съществува абсолютно защитена система. Следователно най-големият враг на администратора е времето. Колкото по-често се извършват проверки и актуализации на защитните механизми, толкова по-малка е вероятността нападателят да успее да използва съществуваща уязвимост.
Макар че съвременните инструменти за анализ на риска значително улесняват процеса на управление на сигурността, практиката показва, че технологичните решения сами по себе си не могат да гарантират необходимото ниво на защита.
Сигурността трябва да се основава на цялостен модел на управление, тъй като не е възможно да бъдат предвидени всички потенциални рискове и комбинации от действия, способни да доведат до инциденти.
Особено трудно предвидим фактор остава човешкото поведение.
Сред най-важните предпоставки за успешното внедряване на политика за сигурност са:

- активната подкрепа от страна на ръководството;
- участието на всички заинтересовани страни;
- непрекъснатото обучение на потребителите;
- редовният преглед и актуализиране на политиките и процедурите.

С нарастващата зависимост на организациите от информационни и комуникационни технологии, те все по-често се превръщат в обект на атаки от страна на киберпрестъпници. Следователно организациите трябва непрекъснато да подобряват механизмите за защита на своите ресурси.
В заключение може да се посочи, че абсолютна сигурност и нулев риск не съществуват. Единствената реалистична цел е уязвимостите да бъдат сведени до възможния минимум.
Навременното актуализиране на системите за сигурност, използването на съвременни защитни технологии и наличието на компетентен и опитен администратор представляват ключови предпоставки за успешната защита на информационните системи.
Колкото по-голямо е участието на човешкия фактор в дадена система, толкова по-голяма е вероятността от възникване на риск.
Следващата глава е посветена на електронното управление, което представлява основа за модернизацията и развитието на публичния сектор.

ГЛАВА 3: ЕЛЕКТРОННО УПРАВЛЕНИЕ (E-GOVERNMENT)

Електронното управление е неразделна част от ежедневието на гражданите. То оказва влияние върху техните навици и социално поведение, като същевременно поставя пред публичната администрация необходимостта да се адаптира към

бързото развитие на технологиите и да премине към една нова цифрова ера. Успехът на този преход зависи от колективното сътрудничество на местно, регионално и национално равнище, както и между държавите членки на Европейския съюз. Цифровата публична администрация допринася за преминаването от тромава и неефективна държавна система към администрация, ориентирана към гражданите и техните потребности. Гарантирането на свободата на изразяване и защитата на личния живот на гражданите представляват основни задължения на съвременната държава.

Публичният сектор в Гърция със закъснение се стреми да въведе необходимите промени за цифровата ера, като същевременно се сблъсква с редица проблеми, които се задълбочиха по време на икономическата криза. Технологиите допринесоха значително за компютъризацията на административните услуги и се възприемат положително особено от по-младите служители в публичната администрация. Използването на цифрови технологии подпомага реорганизацията на административните процеси, повишава ефективността и качеството на услугите и съдейства за утвърждаването на принципите на доброто управление.

Политическата воля на всички нива представлява основно условие за насърчаване на иновациите и реализиране на цялостна цифрова администрация. Необходимо е също така служителите да бъдат обучавани и мотивирани за използването на електронни услуги, да се преодолява съпротивата срещу промените и да се гарантира цифровото включване на всички граждани без изключение.

Електронното управление е призната в световен мащаб необходимост. То играе водеща роля във всички форми на сътрудничество, организация и управление както в публичния, така и в частния сектор. Под понятието електронно управление се разбира използването на информационни и комуникационни технологии с цел подобряване на услугите, предоставяни на гражданите, бизнеса и публичните институции. Електронното управление се развива непрекъснато и допринася както за подобряване качеството на публичните услуги, така и за по-ефективна комуникация между държавата и обществото.

Следователно електронното управление представлява форма на развитие на публичната администрация, която позволява двустранна комуникация между институциите и гражданите чрез използване на информационни технологии, цифрови инструменти и телекомуникационни средства. То проправя пътя към предоставянето на държавни услуги чрез интернет, като едновременно с това повишава прозрачността и ефективността на административната дейност. По този начин отпада необходимостта гражданите да посещават физически административните служби за извършване на голяма част от административните процедури.

Развитието на телекомуникациите и интернет създаде нов тип общество с високи очаквания и нарастващи изисквания към публичния сектор. В същото време държавата осъзнава, че внедряването на цифрови технологии допринася за решаването на важни административни проблеми и подпомага изграждането на нов тип взаимоотношения между администрацията, гражданите и организациите.

Развитието на информационното общество, разширяването на мрежовите инфраструктури и дигиталната трансформация съществено повишават производителността и намаляват бюрократичните пречки.

Електронното управление може да бъде определено като използване на информационни и комуникационни технологии в публичните институции, съчетано с организационни промени и развитие на нови компетентности сред служителите. Основната цел е подобряване качеството на публичните услуги, укрепване на демократичните процеси и подпомагане на политиките, реализирани в полза на гражданите. Поради това електронното управление е сред стратегическите приоритети на Европейския съюз.

Развитието на Европа до 2030 г. е свързано с изграждането на силна, конкурентоспособна и технологично напреднала икономика. Европейският съюз се стреми да бъде равностоен партньор на водещите световни икономики, като инвестира в човешки капитал, иновации и модерни технологии. Визията за Европа включва създаването на общество, основано на сътрудничество, устойчиво развитие и ефективно използване на ресурсите.

Европа на 2030 г. ще има активна роля на световната политическа сцена и ще участва активно в реформите на международните институции, включително Световната търговска организация. Същевременно ще продължи усилията си за справяне с глобални предизвикателства като изменението на климата, опазването на околната среда и развитието на цифровата икономика.

Особено значение ще има защитата на киберпространството. До 2030 г. Европейският съюз

ще разполага с по-добре координирани механизми за противодействие на киберзаплахите и киберпрестъпността. Защитата на държавните информационни системи ще бъде гарантирана чрез съвременни законодателни рамки и обща политика за сигурност и отбрана.

По отношение на Гърция следва да се отбележи, че след продължителен период на икономическа криза и стагнация икономиката все още среща трудности по пътя към устойчив растеж. Въпреки това цифровата трансформация и развитието на електронното управление могат да допринесат съществено за модернизацията на публичния сектор и за повишаването на неговата ефективност.

Непрекъснатите промени в информационните технологии и развитието на интернет налагат необходимостта от постоянно наблюдение и анализ на процесите, свързани с електронното управление. Широкото приложение на интернет технологиите превърна електронното управление в обект на изследване от множество научни дисциплини, включително информатика, икономика, публична администрация, политически науки, социология и право.

Основната цел на програмите за електронно управление е повишаване качеството на публичните услуги чрез намаляване времето за административно обслужване, подобряване на комуникацията с гражданите и повишаване ефективността на държавните институции.

Електронното управление представлява инструмент за изграждане на нови взаимоотношения между държавата и гражданите чрез модернизиране на процедурите и подобряване на комуникацията между

публичните институции. Това се постига чрез осигуряване на оперативна съвместимост и взаимна свързаност между информационните системи на публичния сектор. Резултатът е по-бързо, по-икономично, по-прозрачно и по-сигурно административно обслужване.

През последните години Гърция отбеляза напредък в развитието на електронното управление. Независимо от това постигнатите резултати все още не са достатъчни, за да достигне нивото на водещите държави в Европейския съюз. Страната продължава да се нуждае от мерки за намаляване на административните разходи, повишаване на производителността на публичния сектор и увеличаване на прозрачността.

Следователно Гърция трябва да засили усилията си за развитие на електронното управление с цел ограничаване на бюрокрацията, намаляване на разходите, повишаване прозрачността и укрепване на демократичните процеси чрез по-активно участие на гражданите в управлението.

В заключение може да се отбележи, че електронното управление представлява основата за бъдещото развитие на публичния сектор. Както в Европа, така и в Гърция то се разглежда като ключов фактор за изграждането на модерна, конкурентоспособна и ефективна администрация, способна да отговори на нуждите на гражданите по бърз, достъпен и качествен начин.

Електронното управление е бъдещето на публичната администрация. То предоставя възможност на хиляди граждани да получават услуги по-бързо и по-ефективно, като по този начин укрепва тяхната роля в съвременното общество.

ГЛАВА 4: СЪВРЕМЕННИ ТЕХНОЛОГИИ – CLOUD COMPUTING – G-CLOUD

Едно от най-значимите развития в областта на информационните технологии през последните години е навлизането и бързото разпространение на облачните изчисления (Cloud Computing). Този термин описва съвременна технологична концепция, възникнала в резултат от сближаването на информационните технологии и телекомуникациите. Облачните услуги традиционно се представят графично под формата на „облак“, което символизира факта, че потребителят не се интересува от вътрешната архитектура и начина на функциониране на системата, а единствено от възможността тя да предоставя необходимите услуги по надежден и ефективен начин.

По своята същност облачните изчисления представляват съвкупност от изчислителни системи, способни да приемат заявки чрез телекомуникационни мрежи, да обработват необходимите задачи и да връщат резултатите към потребителя чрез същите комуникационни канали. По-конкретно, терминът се отнася до изчислителни среди, които използват споделени ресурси като мрежи, сървъри, устройства за съхранение на данни, приложения и различни услуги.

Тези ресурси са достъпни чрез високоскоростни телекомуникационни връзки, които позволяват едновременното изпълнение на голям брой изчислителни задачи. По този начин се променя традиционният модел на използване на

компютърните системи, тъй като вече не е необходимо всяка организация да изгражда и поддържа собствена физическа инфраструктура за покриване на своите изчислителни нужди.
Вместо това необходимите ресурси се предоставят чрез интернет от централизирани центрове за данни (Data Centers), които разполагат със значителна изчислителна мощност. Услугите се предоставят съгласно модел, при който клиентът заплаща само за реално използваните ресурси. Този модел осигурява висока степен на гъвкавост и позволява динамично увеличаване или намаляване на ресурсите според потребностите на организацията.
Една от най-важните характеристики на облачните технологии е именно тяхната мащабируемост. Когато потребностите на дадена организация нараснат внезапно или варират във времето, облачната инфраструктура може да се адаптира незабавно без необходимост от закупуване на допълнително оборудване.
Според информацията, публикувана от Генералния секретариат по информационни системи на Гърция, държавната облачна инфраструктура G-Cloud е разработена в съответствие с международния стандарт за информационна сигурност ISO 27001, който гарантира високо ниво на защита при управлението на виртуалните инфраструктури. Освен това системата е съобразена със стандарта ISO 20000 за управление на ИТ услуги, който осигурява определено и договорено ниво на предоставяните услуги.
Предоставянето на тези услуги се подпомага от съвременни системи за мониторинг, отчитане, управление на споразумения за ниво на обслужване

(SLA), фактуриране и контрол на производителността.
По-специално, Планът за действие за електронно управление 2014–2022 предвижда редица действия за изпълнение на Националната стратегия за електронно управление и Стратегията за административна реформа. Основната цел на този план е да осигури икономия на ресурси, устойчивост на реализираните проекти и стриктно спазване на принципите на електронното управление.
В рамките на този план е включена и инициативата за разработване на стратегия за развитие на държавни облачни услуги (Greek GCloud Strategy) за нуждите на публичната администрация. Основната цел на тази стратегия е по-ефективното използване и управление на информационните системи в публичния сектор чрез прилагане на всички възможности, предоставяни от облачните технологии.
Стратегията предвижда определяне на видовете облачни услуги, които ще бъдат разработвани, условията за предоставяне на приложения като услуга (Software as a Service – SaaS), както и институциите, които ще участват в реализирането на проекта. Особено внимание се отделя на въпросите, свързани със сигурността на информацията, устойчивостта на инфраструктурата и разработването на стратегии за възстановяване при бедствия и аварии.
Една от основните цели на G-Cloud е споделеното използване на изчислителни ресурси между институциите на публичната администрация. Това позволява значително намаляване на разходите за поддръжка на инфраструктурата, по-добро използване на наличните ресурси и повишаване на

ефективността на държавните информационни системи.
Същевременно се определят стандартизирани услуги, които могат да бъдат използвани от всички държавни институции. Определят се и конкретни показатели за качество на предоставяните услуги, както и механизмите за разпределяне на разходите между отделните организации според степента на използване на общата инфраструктура.
Особено важно място в облачната среда заемат Споразуменията за ниво на обслужване (Service Level Agreements – SLA). SLA представлява договор между доставчика и потребителя на услугата, който ясно определя задълженията и отговорностите на двете страни.
Чрез SLA се гарантира минимално ниво на предоставяните услуги и се определят параметри като:

- изчислителен капацитет;
- време за реакция на системата;
- наличност на услугите (uptime);
- процедури при прекъсване на услугата;
- възстановяване на данни;
- компенсации при неизпълнение на договорените условия.

Тези договори са разработени така, че да обхващат подробно всички възможни сценарии, които могат да възникнат по време на използването на услугите. По този начин се избягват неясноти, правни спорове и финансови загуби за участващите страни.

Бъдещето на облачните технологии

Нарастващото приемане на облачните услуги както от частни потребители, така и от организации и държавни институции показва, че тази технология ще продължи да се развива динамично и през следващите години.
Световната икономическа нестабилност и постоянният стремеж към намаляване на разходите превръщат облачните решения в особено привлекателна алтернатива за организациите. Вместо значителни инвестиции в собствена инфраструктура, те могат да използват необходимите ресурси при значително по-ниски разходи и по-висока ефективност.
Въпреки това съществуват и фактори, които възпрепятстват по-бързото внедряване на облачните технологии. Най-значимите сред тях са опасенията относно сигурността, поверителността и защитата на данните. Липсата на универсални стандарти и различията в националните законодателства също създават предизвикателства пред широкото разпространение на облачните услуги.
Поради тази причина доставчиците на облачни услуги инвестират значителни ресурси в разработването на по-надеждни механизми за сигурност. Очаква се в близко бъдеще да бъдат реализирани още по-съвременни технологии за защита срещу кибератаки, природни бедствия и други потенциални заплахи.
Облачните изчисления се базират на големи центрове за данни, които осигуряват икономии от мащаба, по-ниски разходи за изчислителна мощност и възможност за плащане само на реално използваните ресурси. По този начин организациите

избягват необходимостта от инвестиции в допълнително оборудване за покриване на временни или сезонни потребности.
Освен това центровете за данни се проектират с оглед на максимална енергийна ефективност, което допринася както за намаляване на оперативните разходи, така и за ограничаване на въздействието върху околната среда.
Облачните технологии могат да бъдат реализирани чрез различни модели на внедряване и предоставяне на услуги, като Public Cloud, Private Cloud, Hybrid Cloud, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) и Software as a Service (SaaS).
Независимо от конкретния модел, тази технология продължава да се развива с изключително бързи темпове и се използва от организации с различен размер и предмет на дейност. Това ясно показва, че предимствата ѝ — гъвкавост, ефективност, стратегическа стойност и икономическа изгодност — значително надвишават потенциалните рискове и ограничения.
В заключение може да се отбележи, че облачните технологии представляват един от основните двигатели на цифровата трансформация в публичния сектор. Те предоставят възможност за по-ефективно управление на ресурсите, подобряване качеството на услугите и повишаване сигурността на информационните системи. Именно поради това облачните решения се разглеждат като ключов елемент за модернизацията на гръцката публична администрация и за изграждането на една по-гъвкава, ефективна и устойчива държавна система.

ГЛАВА 5: ИЗВОДИ ОТ ИЗСЛЕДВАНЕТО

Методологичен модел

Тъй като основната цел на настоящото изследване е да анализира сигурността на информационните системи и мрежи в публичния сектор чрез използването на съвременни технологии и да извърши сравнение между настоящото състояние в гръцката публична администрация и международната практика, като най-подходящ научен подход е избран методът на систематичния литературен преглед (Systematic Literature Review).

Систематичният литературен преглед представлява обективен метод в рамките на вторичното изследване, чрез който се идентифицират, анализират и оценяват съществуващите научни публикации относно технологиите за защита на информационните системи и мрежи. Чрез този подход настоящото изследване цели формулирането на предложения за стратегии и интервенции, насочени към подобряване на сигурността на информационните системи в гръцката публична администрация чрез използване на съвременни технологични решения.

Систематичните прегледи често използват статистически методи и метаанализ за обединяване на резултатите от множество изследвания с цел формиране на по-надеждни научни заключения. Поради това те се намират на върха на така наречената „йерархия на доказателствата“, тъй като предоставят по-всеобхватна картина в сравнение с отделните емпирични изследвания.

Систематичният преглед се характеризира с:

- ясно определени цели;
- предварително зададени критерии за подбор на изследванията;
- прозрачна и възпроизводима методология;
- систематично търсене на научни публикации;
- оценка на надеждността и валидността на резултатите;
- систематичен анализ и синтез на събраните данни.

Използването на подобен подход позволява минимизиране на субективността и осигурява по-надеждни резултати, върху които могат да бъдат изградени практически препоръки и управленски политики.

Цел и изследователски въпроси

Основната цел на настоящата докторска дисертация е да изследва съвременните технологии за сигурност на информационните системи и мрежи и възможностите за тяхното адаптиране към нуждите на гръцкия публичен сектор.
В рамките на тази цел се поставят следните изследователски въпроси:

- Да се подчертае необходимостта от използването на защитени информационни системи в гръцкия публичен сектор.

- Да се идентифицират съвременните технологии и тенденции в областта на сигурността на информационните системи.
- Да се определят потребностите на гръцката публична администрация по отношение на сигурните информационни системи.
- Да се подчертае необходимостта от оперативна съвместимост и взаимно свързване на информационните системи в публичния сектор.
- Да се предложат решения за изграждане на защитени комуникационни и информационни мрежи.
- Да се анализира ролята на електронното управление за гарантиране на сигурността и правилното функциониране на информационните системи.
- Да се подчертае значението на законодателството, свързано с прозрачността и доброто управление в публичната администрация.

Основни изводи от изследването

В съвременната епоха публичните администрации са изправени пред нарастващи изисквания за по-ефективно управление на обществените ресурси и предоставяне на качествени услуги. Електронното управление представлява ключов механизъм за модернизиране на държавните институции чрез използването на информационни и комуникационни технологии.

Цифровите технологии днес са неразделна част от ежедневния живот на гражданите и оказват съществено влияние върху функционирането на публичната администрация. Те променят начина на работа на държавните институции и трансформират отношенията между държавата, гражданите и бизнеса.

Въпреки значителния напредък през последните години Гърция все още изостава спрямо повечето държави от Европейския съюз по отношение на степента на цифровизация. Това води до пропуснати възможности за подобряване на ефективността, създаване на нови услуги и ограничаване на административните разходи.

Успешното внедряване на съвременни технологии изисква наличието на политическа воля, подходяща нормативна рамка, достатъчно финансови ресурси и обучен човешки капитал. Особено важно е повишаването на цифровите умения на държавните служители чрез непрекъснати програми за обучение и квалификация.

Особено значение има и необходимостта от оперативна съвместимост между различните информационни системи в публичната администрация. В продължение на години много системи са били разработвани самостоятелно и без общи стандарти, което е довело до сериозни проблеми при обмена на информация между институциите.

Основни проблеми и предизвикателства (Concerns)

В рамките на изследването бяха идентифицирани няколко съществени проблема, свързани с внедряването на облачни технологии в гръцката публична администрация:

1. Липса на публично достъпна стратегия за възстановяване при бедствия

В наличната информация относно държавните облачни услуги липсват достатъчно данни относно съществуващите механизми за възстановяване при бедствия и аварии.

2. Необходимост от сътрудничество с частни доставчици

Липсата на достатъчно резервни механизми поставя въпроса за евентуално сътрудничество между държавата и сертифицирани частни доставчици на облачни услуги.

3. Човешки ресурси

Съществуват опасения относно стабилността на човешките ресурси, ангажирани с управлението на критични инфраструктури и чувствителни данни.

4. Технически персонал

Значителна част от техническите специалисти работят по договори извън държавната

администрация, което поражда допълнителни въпроси относно сигурността и контрола.

5. Софтуерни лицензи

Проблемите, свързани със софтуерните лицензи и виртуализираните среди, могат значително да увеличат разходите за използване на определени приложения в облачна среда.

6. Нормативна рамка

Развитието на облачните услуги изисква ясна и стабилна законодателна основа, която да регламентира тяхното функциониране.

7. Административна приемственост

Честите промени в политическото и административното ръководство могат да доведат до забавяне или прекратяване на стратегически проекти.

8. Задължителна миграция към G-Cloud

Липсва обща стратегия, която да задължи публичните институции постепенно да преминат към използването на централизираните държавни облачни инфраструктури.

Предложения за бъдещи изследвания

Бъдещите научни изследвания могат да бъдат насочени към:

- Анализ на проблемите, свързани със сигурността и поверителността в облачните среди.
- Изследване на законодателните ограничения, които възпрепятстват развитието на глобални облачни пазари.
- Разработване на критерии за определяне кои данни и услуги са подходящи за прехвърляне в облачна среда.
- Анализ на допълнителни практически примери от организации, внедрили облачни технологии.

Принос на докторската дисертация

Основният принос на настоящата дисертация се състои в изследването на ролята на информационните системи в публичната администрация и възможностите за повишаване на тяхната сигурност чрез използването на съвременни технологии.
Изследването показва, че информационните системи:

- подобряват ефективността на държавните служители;
- повишават качеството на административните услуги;
- намаляват бюрократичните процедури;
- улесняват обслужването на гражданите;
- повишават прозрачността и отчетността на публичната администрация.

Особено внимание се отделя на значението на облачните технологии като инструмент за подобряване на сигурността, надеждността и

устойчивостта на публичните информационни системи.

Епилог

Съвременната публична администрация е изправена пред необходимостта от промяна на своята организационна култура и начин на мислене. Държавните служители трябва да възприемат институцията, в която работят, като общност, чието развитие зависи от тяхната активност, професионализъм и готовност за промяна.
Публичната администрация следва да насърчава иновациите, обучението и инициативността, като същевременно създава условия за ефективно управление на рисковете.
Миналите грешки, затруднения и неуспехи не трябва да се разглеждат като пречки, а като ценен източник на знания и опит, който може да подпомогне устойчивото развитие на публичния сектор.
Облачните технологии представляват мощен инструмент за модернизацията на организациите. При правилно използване те могат значително да подобрят ефективността, сигурността и конкурентоспособността както на частния, така и на публичния сектор.

Заключителен коментар

Настоящото изследване показва, че облачните технологии вече не са просто технологична иновация,

а фундаментален елемент от развитието на съвременните информационни системи.
Световни технологични лидери като Microsoft, Google и други инвестират значителни ресурси в развитието на облачните услуги, а институции като Европейския съюз активно насърчават тяхното внедряване чрез политики и финансови програми.
Въпреки че Гърция все още изостава от водещите европейски държави в тази област, потенциалът за развитие остава значителен. За да бъде реализиран този потенциал, е необходимо преодоляване на организационните, технологичните и културните бариери, които продължават да възпрепятстват цифровата трансформация.
В крайна сметка успехът на всяка реформа зависи не само от технологиите, но и от готовността на обществото и институциите да приемат промяната. Само чрез такава трансформация гръцката публична администрация ще може да постигне висока степен на ефективност, прозрачност и устойчиво развитие в условията на цифровото общество на XXI век.

SOUTH WEST UNIVERSITY
"NEOFIT RILSKI"

MARIA CHRISTOS MPITSI

IMPROVING THE SECURITY OF INFORMATION AND NETWORK IN GREEK PUBLIC ADMINISTRATION USING STATE-OF-THE ART TECHNOLOGIES

SUPERVISING PROFESSOR: Nina Sinyagina

ABSTRACT OF DOCTORAL THESIS

BLAGOEVGRAND

2026

THANKS

Before presenting this doctoral dissertation, I consider it necessary to refer to those special people with whom I have had the good fortune to work with throughout this arduous endeavor. I thank them all from the bottom of my heart and I especially thank the supervising professor Nina Sinyagina for her substantial scientific contribution and guidance as well as her material and moral assistance at all stages of the relevant research project. Also, the contribution of my professors Stefan Stefanov and Petrana Stoikova was decisive, to whom I must express my sincere thanks for their great contribution to the completion of my studies.

At the same time, I would like to warmly thank the members of the advisory committee, who devoted a significant part of their valuable time to the study of this dissertation.

Then, I thank my sister friend Anthoula for the overall support and always her good word. I owe a big thank you to my children, Dimitris, Christina - Lemonia, Zoi - Smaragda, Raphaelia – Theophania, Zinaida – Roxane, Myriam – Cleo for their patience for the quality time I deprived them of during my doctoral dissertation. In closing, I thank my comrade Vangelis, for his undivided help, understanding, support he has provided me all these years and the trust in what I have dared to date.

ABSTRACT

Digital technologies are an integral part of everyday life and have a decisive influence on Public Administration and Public Services, shaping the way in which the activities of the Administration are carried out and the daily services offered to the citizens and the private economy.

In modern times, globally, the public administrations of the countries try to reshape and reshape the administrative structures in such a way as to make them more efficient, faster and less costly. This logic includes reform efforts such as the implementation of the New Public Management, a reform which aspired and still aspires to solve the dysfunctions of the public administration by applying logics and practices derived from the private sector.

The category of reform efforts also includes e-Government. It is a philosophy of reforming public services by adopting and using the tools offered by technology. The e-Government therefore concerns the use of technologies by the Public Administration for the execution of its activities but also the communication and the daily transactions with the citizens and the organizations.

In the present study, the interest is focused on issues of information systems operating in the Greek Public Sector using state-of-the-art technologies. The use of information systems in the public sector is imperative and today does not mean any public organization that seeks development without investing in new technologies, without trying to improve its position in the domestic and global market.

Cloud computing is an innovative cutting-edge technology that enables organizations to improve their business operations, serve their customers' needs faster, reduce their costs and become more competitive. In short, it contributes to the added value of the organizations that decide to adopt it.

KEY WORDS:

Information Systems, Management Information Systems, Information Systems and Networks Security, E-Government, Public Administration, State-of-the-art technologies, Cloud Computing.

TABLE OF CONTENTS

Improving the security of the information and networks in Greek Public Administration using state-of-the-art technologies

Chapter 1: INFORMATION SYSTEMS

More than ever, organizations around the world treat information as one of their main resources. Therefore, it is not surprising that information systems are a critical building block of modern organizations and are used to support all kinds of organizational functions and activities.

The literature mentions more than one definition of the term “information system”, which differ more or less from each other. In this thesis, we will define the Information System as an operational system that processes data from the external and internal environment of the organization and provides information to its management, so that quick, correct and valid decisions can be made.

For this thesis, it was chosen to describe the strategic level systems in more detail, as part of them are the public administration information systems that this thesis deals with.

Specifically:

1. Transaction Processing Systems (T.P.S): In organizations, the collection and maintenance of records for daily transactions were two of the first processes that began to be carried out through computers. Thus, with these systems, those processes that are repeated were automated. Transaction Processing Systems provide front-line executives with information related to the basic activities and transactions of the organization. It is a computerized system that executes and records current routine transactions that are necessary for conducting business activity.
2. Management Information Systems (M.I.S.): Middle managers need systems to help them monitor, control, and make decisions in administrative activities. Management Information Systems provide middle management with reports on the current performance of the organization. This information is used to monitor and control the organization and to predict its future performance. In general, MIS provides answers to routine questions that have been identified in advance and there is a predefined process for answering them. A management information system supports the decision-making of organizational executives. These systems produce reports for long-term goals, compared to transaction processing systems that deal with routine processes (Osterle, 2013).
3. Decision Support Systems (D.S.S.): Decision Support Systems support decision-making, mainly by middle managers, that is not routine. These systems combine data, processed analytical models and user-friendly

software into a single powerful system that can support semi-structured or unstructured problems. They focus on problems that are unique and change rapidly, and for which the solution process cannot be fully specified in advance. Decision support systems deal with problems that are not planned, but which require the critical intervention of the manager, while management information systems deal mainly with problems that are planned and with routine decisions. Furthermore, a decision support system does not rely only on internal information from the transaction processing system, as the management information system typically relies on. In contrast, a decision support system is structured to absorb new external information into the analysis (DaSilva & Reikman, 2014). D.S.S. are designed so that users can work directly with them, as they include user-friendly software. Sometimes these systems are called Business Intelligence Systems, because they focus on helping users make better business decisions (Laudon & Laudon, 2009, pp. 55-57).

4. Executive Support Systems (E.S.S.): Executive support systems are information systems designed to help senior executives obtain, manipulate, and use the information they need to maintain the overall effectiveness of the organization. These systems often focus on providing senior management with information for strategic decision-making. They help senior management deal with changes in the environment, taking into account the strengths and weaknesses of the organization.

ESSs deal with unstructured problems that require judgment, evaluation and intuition, because there is no agreed-upon process for reaching a solution. Management Support Systems are designed to integrate data about external events, but also draw information from internal MIS and DSS. They filter, summarize and monitor critical data, presenting those that are of greatest importance to senior management.

5. Expert Systems (ES): Expert Systems (ES) are a type of information system that refers to specialized areas of human knowledge and is developed based on the knowledge of experts to solve problems that normally require human knowledge and experience. That is, they are systems that imitate the way in which executives of organizations make their unstructured decisions. In order to provide an answer to a problem, the information for which is usually uncertain, unclear or even incomplete, Expert Systems use heuristic methods to quickly find a satisfactory solution, which is not necessarily the optimal one (Eikonomou & Georgopoulos, 1995, p. 95).

The strategic systems that we have just described are interdependent. TPSs are generally the main source of data for other systems, while ESSs are primarily recipients of data from lower-level systems. Other types of systems can also exchange data with each other.

In conclusion, each organization, by studying its internal and external environment and detecting strengths, weaknesses and opportunities, threats respectively, shapes its strategy. The formulation of the strategy is followed by

its implementation and finally the evaluation and control of the actual results, in order to identify possible deviations in relation to the desired results and to plan the appropriate corrective actions.
In this effort, Information Systems can play a special role. In conclusion, the choice of the right ERP and its correct implementation are the points that give the competitive advantage to the organization and not the ERP system itself (Sfyris, 2017).
Information systems in combination with new technologies can make an organization more efficient, effective but also more innovative in the production of services. Of course, in order for an organization to reap these benefits, new technologies and information systems must be implemented in such a way that they are in harmony with the organization's goals.
Technology today constitutes the basis for the development of the organization, technology does not stand still, it advances, and especially at the level of serving citizens, new technologies are necessary, since their existence simplifies the communication of the public organization with citizens, improves internal and not only processes, and provides speed to service. Continuous modernization is necessary, without it there can be no future.
The problem of information system security is particularly acute in our days. The ever-increasing use of technologies, based on databases and networks, as well as the important role of information systems in an organization, make it necessary to take security measures to protect their information.
The concept of information systems security is related to the ability of an organization to protect its information from any alterations and destruction, as well as from unauthorized use of its resources.
Information systems security is related to a) prevention, which includes measures to prevent possible damage to the components of an information system, b) detection, which includes the search for when, how and by whom damage was caused to a component of an information system and c) reaction, which includes the restoration or recovery of the components of an information system.
The concept of information systems security is closely linked to three fundamental concepts: a) confidentiality, b) integrity and availability. In addition to these, the following are equally important: a) authorized use, where authorized individuals can always use the information system in accordance with the predetermined manner, b) message authentication, i.e. the certainty that the individual sent the message in accordance with the system, c) non-repudiation, the certainty that the message has found its recipient, d) accountability, where users are responsible for their actions, and f) reliability and safety, as a prerequisite for the proper functioning of systems even under adverse conditions.
However, the information system is vulnerable to vulnerabilities. By the term vulnerability we mean a weakness or a vulnerable point in the security

system, which can become the object of an attack for the system. A categorization of vulnerabilities includes: physical vulnerabilities, natural vulnerabilities, hardware and software vulnerabilities, communications vulnerabilities, and human vulnerabilities.

A threat to an information system is any situation that can cause damage or loss, such as human attack or unintentional human errors, natural disaster or even internal imperfection of equipment or software. The types of threats to the resources of the information system in relation to hardware, software and data are: interception, modification, fabrication and interruption.

In order to limit vulnerabilities and threats in an information system, protection measures (controls) should be foreseen and implemented. Protection measures or countermeasures are the procedures, techniques, actions and devices that limit the vulnerabilities of an information system. The different types of countermeasures result in the analysis of the problem of information system security in the components of physical system security, computer system security, database security and network security.

There are various types of protection measures to prevent the exploitation of vulnerabilities in an information system. The most characteristic are, cryptography (encryption), i.e. the coding and scrambling of messages, is a widely used technology for securing electronic transmissions in unprotected networks (Wallace, 2014). Also, software controls, hardware controls and security policies (Pangalos & Mavridis, 2002).

As people place great emphasis on productivity, they may neglect security if it is an obstacle to achieving it. The social machine exploits people's behavioral tendencies with the aim of manipulating them into revealing sensitive information or bypassing security measures. Security awareness training, as well as awareness of the relationship between security, ethics and privacy, can help address these tendencies (Wallace, 2014).

Summarizing this chapter, it is understood that information systems are essential for the development and operation of public services. The information systems that were chosen to be presented are the strategic level systems as part of them are the public administration information systems that are discussed in this thesis. Their use in the public sector is also mandatory and today there is no public organization that seeks development without investing in new technologies, without trying to improve its position in the domestic and global market. The Greek state, which has been based for many years on a bureaucratic model, needs to change its current form and operation, by investing in new technologies, in models that will help it develop, reduce the problematic situation it has been experiencing for many decades and develop dynamically. Especially during the years of crisis, new technologies can help it reduce costs while at the same time improving the quality of its services provided. The next chapter will continue with the security of information systems.

Chapter 2: INFORMATION SYSTEMS SECURITY

In recent years, there has been a rapid development in the development of information systems. Many public and private sector organizations rely on the existence of information systems. Using these systems on a daily basis, they exchange information, offer and develop services by transferring large volumes of data. The security of information systems is a critical factor for the operation and viability of an organization. The slightest malfunction, interruption and illegal intrusion into information systems have the impact of causing financial losses and even the inability of the organization to function smoothly. Furthermore, the most serious security problems of information systems are more focused on those systems where sensitive data, information and important functions are recorded. In order to achieve security, appropriate measures need to be implemented against the various threats they may receive.

The problem of information systems security has always been critical since the beginning of information technology. Undoubtedly, today the risk is more conscious, as systems are exposed to a wide range of users and therefore risks. Information, whatever its form, if it is important, needs to be stored correctly and protected appropriately. In short, the ultimate goal of information security is to protect information from a wide range of threats.

We could say that if security is likened to a pyramid, then certainly the basis for this is the design and implementation of a comprehensive security policy. It is essentially the basic tool for managing the security of information systems despite the fact that the term “Security Policy” can have different meanings depending on the purpose, form, type of policy and the environment in which it is applied (Karyda, 2005).

The design of Security Policies is directly linked to technical procedures and administrative measures adopted to protect information systems from any kind of accidental or deliberate threat. The most important point in their design process is the identification of the information that must be used and protected as well as the risk analysis - risk assessment.

The security policy is applied to understand the following questions:

- What is the goal and purpose of the policy?
- What are the system assets that need protection?
- Who is responsible for the protection of the assets and what are their responsibilities?

The security of information systems is very important as it is based on three basic conditions for its proper functioning, a) integrity, b) availability and c) confidentiality. Addressing security problems, although not a simple matter, must be taken seriously. The introduction of information systems into an environment can significantly increase productivity and profit, but it introduces new risks that significantly increase the risk and therefore must definitely be

recognized and dealt with accordingly (Elky, 2006). The information systems security industry fortunately has to offer a multitude of countermeasures (tools, methods, controls, security policies) to address any type of problem. However, integrating all of these into each organization is not at all a simple matter. On the contrary, the different way of operating as well as the different assignment of resources for security issues create completely different conditions, unique to each organization. Security integration should not be considered a simple process, as all factors must be taken into account at all times so that security does not become an obstacle to the operation of the organization but serves it (Karnavas, 2012).

Risk analysis provides a solution to this problem. Risk analysis aims to evaluate the assets of the organization and identify all the risks and vulnerabilities that threaten them. It should be mentioned at this point that the term “assets” does not only mean purely financial figures. On the contrary, values such as personal data, data whose violation can lead to the loss of human life, the image of an organization to the outside world, etc. are also included. With this data, the risk introduced by the use of each information system in the operation of the organization can be calculated. Thus, it can be calculated with satisfactory accuracy which countermeasures are advantageous to install and in which cases it is preferable to accept the risk.

Additionally, risk analysis prioritizes countermeasures that can be implemented, resulting in a more appropriate choice in cases where the budget does not allow for sufficient resources to cover all security needs. Especially today, when the global economy is in recession and most businesses and organizations are forced to make cuts in all areas, risk analysis comes to play an essential role in properly addressing security problems in an organized and effective manner.

In conclusion, the goal of a security policy system is to limit risk. The system includes risk assessment and limiting the acceptable level of security, developing and implementing a security policy as well as creating an appropriate organizational framework and ensuring the necessary resources for the implementation of the security policy. The security policy together with all the protection measures constitute the security plan for the information systems of an organization, because a comprehensive framework with the guidance of security measures is needed to function as a means of communication between those involved in security issues.

The choice of a risk management technique - methodology depends on the specific characteristics of the information system to which it is to be applied, as well as on economic and organizational factors. Some of the criteria for selecting a risk analysis and management technique (Kokolakis, 2000): a) it should correspond to the size and complexity of the information system, b) it should have low implementation costs, c) it should fit the organizational characteristics and culture of the organization, d) it should be supported by specialized software, e) the persons who will be called upon to apply it should

have experience in its application or at least have been trained in it and f) it should cover all the factors (technical and social) associated with the security of information systems. We conclude that, through the protection measures, the important role of the security officer, who has the appropriate knowledge on security issues and is selected by the organization's management for this specific purpose, is clearly evident.

The vast range of attack tools and users willing to use them constitute a major obstacle to system security, making these tools the only safeguard one can look for to ensure the best possible shielding of information systems. History has proven that any security system can be breached, so the greatest enemy of any administrator is time. The more often holes in an information system are checked and the better they are closed, the less risk is minimized and the less time the attacker has to start over.

Although nowadays the risk analysis process is greatly facilitated by the existence of relevant software, which provides important advice and guidance for a significant level of security, it has been empirically proven that mechanisms and techniques alone do not constitute security measures. These must operate according to a security model, as it is impossible to predict the risks in any of our actions, in the sense that the possible combinations of actions that are likely to cause problems are infinite with human nature being the most difficult factor.

Some important factors for the successful implementation of the security policy are the participation and support of the organization's management and its universal implementation by all stakeholders of the system. In addition, the security policy should also be accompanied by user education and information processes and should be regularly reviewed for both its content and its implementation. As IT and networking resources have become increasingly an integral part of organizations, they have also become a target for criminals. Organizations must be careful in how they protect their resources.

In conclusion, it is not possible to have absolute security and zero risk. The only thing the defender can do is try to reduce the system's vulnerabilities to zero. Also, an important factor is the timely updating of security systems so that the system administrator can prevent an ambitious attacker using the latest exploits and the most recent updates to attack tools. Tools are a very good option for continuous and regular monitoring of an information system, but they cannot guarantee security by themselves. Every system must have a responsible, experienced, available and insightful administrator who is available to prevent any possible threat. Ultimately, the more the human factor is included, the greater the risk. The next chapter studies e-government, which is the basis for the development of the public sector.

Chapter 3: E-GOVERNMENT

E-government is in the citizen's everyday life. It affects his habits and social behavior. Public administration is called upon to keep up with the rapid developments in technology by moving more quickly into a digital era. Success lies in collective cooperation at local, regional and national levels, as well as between member states. Digital public administration contributes to the transition from an inflexible and inefficient public administration focused on the state, to an administration with the citizen as its central point of reference and the provision of services to satisfy their needs and desires. Respect and ensuring freedom of expression and the protection of the citizen's privacy are essential obligations.

The public sector in Greece is belatedly trying to promote the necessary changes for the digital era, with several problems that intensified with the economic crisis. Technology has contributed significantly to the computerization of administrative services and is viewed positively by younger public administration executives. Digital technology in public administration contributes to the redesign of procedures, the effectiveness and efficiency of services and good governance. Political will at all levels is a necessary condition for promoting innovations and actions for an integrated digital administration, inspiring all those involved in the processes with appropriate education and training, aiming at changing the mindset for the use of e-government services and eliminating resistance to change, aiming at the digital inclusion of all citizens without exclusions.

E-government is a globally recognized need. It plays a leading role at all levels of cooperation, organization and administration, whether we are referring to the private or public sector. It includes the use of Information and Communication Technology with the aim of improving services to citizens, businesses and other public services. E-government is developing and can help on the one hand to improve the services provided and on the other hand to improve communication with citizens. It can also help with immediacy and service. Therefore, e-government is a point of development of administration that allows for a two-way relationship with other bodies, the use of information technology, digital tools and telecommunications. It marks the path towards the provision of government services via the internet but also the enhancement of the transparency and effectiveness of the work of public administration with the aim of recognition and acceptance by citizens. Therefore, e-government defines a new concept in the service of citizens and businesses by public services, since it eliminates the need for the citizen to physically travel and be present in local public services.

The evolution of telecommunications and the development of the Internet create a new civil society with high expectations and demands. On the other hand, the state understands that the adoption of digital technology solves

important administrative problems and helps to redefine relationships with citizens or organizations. At the same time, the development of the information society, the expansion of networks and the IT revolution improve productivity and simplify bureaucratic procedures.

Electronic government (e-Government) is defined as “the use of ICT in public services (central and regional, central administration or local government), in combination with organizational changes and new skills of staff. The aim is to improve the provision of public services, as well as to strengthen democratic processes and support for policies implemented by the public sector for the benefit of citizens. E-Government is among the important priorities of the European Union.”

The differentiation of Europe - Greece with a horizon of 2030 focuses on the strong, on the one hand, agenda of Europe and the weak, on the other, unoriented agenda of Greece. A Europe with political, economic and technological skills, an equal partner of strong economies around the world, with a productive potential harmonized in the utilization of resources and capabilities, in the upgrading of a highly qualified and educated human resource that faces the challenges of the future. A Europe based on bridging relationships of respect and mutual interest, which occupies a leading position in a global network of free trade based on principles and rules that deter all forms of protectionism, and which also enjoys the benefits of the global nature of international trade with multiplying, added energy for businesses, consumers and workers.

Europe in 2030, open to the world, with a strong voice on the global political scene, will contribute to the comprehensive reform of the World Trade Organization, will negotiate with arguments and will have direction in the reform agenda of changes, at all levels of social, political and economic life.

An active leader in the challenges that come and in a privileged position, securing global agreements on the major, controversial issues: climate change, environmental protection and its participation in the demands of the digital economy. Ensuring the integrity of the European Union's single market and the existence of a safety net with the United Kingdom is a priority for a deep economic and political relationship. The long-standing alliance with the USA and Canada will oppose potential obstacles that create turbulence in commercial mobility and investment. The threat to democracy that raises awareness and mitigates adversities is a priority on the 2030 agenda, while deeper partnerships with neighboring countries, depending on the specificities of each state, are a sign of political culture and rational political behavior. Relations with Russia will evolve in the logic of reciprocity and respect for international rules, and on the other hand, its relationship with African countries will be delimited within the framework of beneficial economic relations and free trade between the two continents. The participation and organization of regional and global supply chains and investments in basic infrastructure will function preparatoryly in an environment of innovation and a

balanced development process. Everyone now understands that competition on equal terms and the expansion of areas of cooperation constitute the only path to sustainable prosperity.

The influx of illegal immigration will also be controlled to a large extent through an effective security system for the external borders of the European Union. But in 2030 Europe will also dominate cyberspace around the world, through a necessary coordination for any threats in this area as well as taking measures that limit crime. External threats and the security of state entities will be protected on the basis of agreed rules and a serious legislative framework that ensures functionality and effectiveness within the framework of a common security and defense policy.

And all this, of course, contradicts the unfavorable predictions of Br. Simms, a Cambridge professor, for Europe in a recent publication in the New Statesman, who argues that a new period is opening, corresponding to that of the early 16th century, of fragmentation and acute political and ideological confrontations within states, which is unknown when it will close.

Now regarding Greece, it is true that after almost a decade of introversion, contraction and stagnation, the economy remains weak and anemic. Under normal circumstances, the ten-year economic crisis should have accelerated the pace by 5% to 7%, but instead it remains stuck at 1.5% to 2%, and forecasts until 2025 range around 2%-2.5%.

The continuous reorganizations in the global IT environment and especially the change in the terms and conditions of the maturation of the Internet make it more imperative to monitor and examine the development of e-government from the contemporary bibliography and articles. The above finding is attributed to the breadth and size that the evolutionary course of the Internet has progressively given to the issue of e-government, a fact that has prompted a multitude of approaches from scientific areas (informatics, technology, economics and administration, politics, sociology, medicine) to engage in creating diverse knowledge.

The aim of implementing e-government programs is to improve the quality of public services provided by governments, which will be measured by specific indicators such as reducing the time for processing procedures and improving service to citizens.

E-government is the "tool" for implementing the new relationship of modernization between citizens and the state, improving procedures, communication between public services, agencies and organizations. This is achieved by focusing on issues of interconnectivity and interoperability of public sector information systems, resulting in faster, more economical, transparent, safer and qualitatively upgraded service to citizens. The digitization of the huge volume of information held by central, regional and local authorities provides the opportunity for more effective and rational administration.

In recent years, Greece has made progress in terms of e-Government. However, the progress made by Greece is not sufficient to reach the level of the European Union countries, despite its needs to reduce operating costs, increase productivity and efficiency of the public sector, as well as increase transparency.

Greece presents the lowest percentage (10%) of electronic transactions, to which only the two well-known services provided by TAXISnet, related to the submission of electronic income tax and value added tax returns, contribute. While it is worth emphasizing the satisfactory position and perspective of Greece, which seems to provide sophisticated and reliable e-government applications.

Greece, therefore, must intensify efforts to develop e-Government in order to reduce costs and bureaucracy, increase transparency, and strengthen Democracy, through increased citizen participation in Governance.

Closing this section, it was found that e-government is the basis for the future development of the public sector. Today, in Europe and in Greece, e-government is the basis for the development of a competitive and integrated public sector, which has the ability to compete with the private sector, while at the same time has the ability to meet the needs of citizens much more easily, much more dynamically.

E-government is the future. As already analyzed above, it covers the needs of thousands of citizens by giving them the opportunity to be served more directly and more effectively. This process strengthens the position of the citizen in today's society.

In the next chapter, as a natural continuation of this, reference will be made to the use of cutting-edge technologies in public sector administration.

Chapter 4: STATE OF THE ART TECHNOLOGIES – CLOUD COMPUTING – Gcloud

A very important development in the field of IT applications that in recent years has been taking on ever greater dimensions, in terms of its use and importance, is cloud computing. This term describes a modern development that became possible due to the convergence of the fields of information technology and telecommunications. Cloud computing is represented in diagrams as a cloud, which shows that the interest is not focused on how it works and from which components it arises. On the contrary, the user is interested in the fact that it "is there" and is able to serve his needs and requirements.

In general, the cloud refers to a set of computing systems that are capable of receiving requests via telecommunications networks, performing the requested tasks and returning the result via the same networks. More specifically, the term refers to computing systems that use shared resources consisting of networks, servers, data storage units, applications and services. These systems are accessed via high-speed telecommunications interfaces, which enable them to receive and execute large volumes of computing tasks simultaneously. This technology is drastically changing the model of computer usage as the need to install and operate individual computing systems within the same physical space in order to meet the requirements for computing tasks no longer exists. Computing needs are transferred via telecommunications interfaces, and in particular via the Internet, to a central hub where significant computing power has been concentrated. There, the task can be served with a guaranteed level of operation, by a service provision model where the customer pays a price proportional to the resources used to execute it. As the demand for work can grow rapidly or fluctuate over time, it must be possible for the capacity to service to grow as well. This is another very important feature that cloud technology offers.

The General Secretariat of Information Systems states on its website that its Gcloud (government cloud) has been designed based on the ISO 27001 security standard, which ensures a high level of security in the management of the virtual infrastructures provided, as well as on the ISO 20000 standard IT service management system, ensuring an acceptable, specified and agreed level of IT services provided. The provision of these services is supported by the use of modern reporting applications, SLA monitoring, invoicing, etc. In particular, the 2014-2022 e-Government Action Plan presents the actions required for the implementation of the 2014-2022 e-Government Strategy and the Administrative Reform Strategy. The main concern of the Plan is to ensure resource savings, the sustainability of the proposed projects and, more generally, the strict adherence to the general principles of the e-Government Strategy.

Finally, with regard to cloud computing services, the action was included: “Development of a strategy for the development of government cloud computing services (Greek GCloud Strategy) for Public Administration”. The purpose of the action is to develop a strategy for the better exploitation and management of Public Administration information systems, using all the possibilities offered by GCloud technology. In addition, it is planned to examine issues such as the identification of the cloud services to be developed, the terms under which an application will be provided as a service, as well as the bodies that will be involved in the project. When preparing the strategy, issues related to information security (infrastructure, disaster strategy, etc.) will be taken into account. A further objective of the action is to achieve shared use of computing infrastructures by Public Administration bodies, with a consequent reduction in the cost of infrastructure maintenance and support, as well as an increase in the degree of utilization of existing or future infrastructures (Gcloud). In addition, the action will establish the standardized services that will be provided to bodies at the level of computing infrastructures. At the same time, the quality levels of provision of these services will be established and the burden on each body's budget for the services it utilizes in relation to the shared computing infrastructures will be calculated. Finally, the method of administering these shared computing infrastructures in relation to the infrastructures, applications and data that will be hosted in them will be designed.

The SLA contract is an agreement concluded between the provider and the user and records the obligations of both parties. Furthermore, it certifies a minimum level of services that the provider will provide to the user. Through this contract, the user receives the necessary guarantees for the proper functioning of the service and for the strength of the features promised by the provider. Although the provisions of the various agreements that can be offered to a prospective user may differ significantly from service to service and from provider to provider, the main points are the same and concern issues such as the computing capabilities of the service, the speed of response, the uptime, the provisions in the event of interruption of the service or in any other case of irregular provision, etc.

SLA contracts are drawn up in such a way as to cover in detail every event that may occur during the use of the service. The reason is obvious, nothing is left to chance and to the subjective interpretations of one or the other side in the event of an unfortunate event. Thus, uncertainties, long-term litigation, irreparable business damage, wasting valuable resources on unproductive processes are avoided.

Cloud technology in the future

The penetration and acceptance of cloud services by both private users and businesses and organizations, demonstrates that this technology will remain in the spotlight for a long time to come, even showing significant growth trends.

The economic crisis that has plagued the global economy in recent years, combined with the relentless trend to reduce costs and make better and more efficient use of available funds, makes cloud services particularly attractive. Given that economic imbalances and instabilities do not seem to recede in the near future, the importance of the financial benefits offered by the use of cloud services will make them a dominant choice if not the only way for businesses.
While optimizing the use of financial resources may push businesses to adopt cloud service solutions, uncertainty in the security sector and the lack of standards still constitute a restraining factor for the adoption of the technology. Significant weight will be given by providers to convince users of the integrity of the services they offer. As long as the latter are convinced of the realism of factors such as uptime, speed, security measures, etc., there is essentially no reason for businesses not to migrate to the cloud. In particular, regarding the issue of security, in the near future more funds are expected to be invested by cloud service providers in order to ensure more robust security against any type of threat, natural or malicious. In summary, this technology has developed rapidly, managing to evolve from a simple internal system for IT departments into a public service, from a simple cost-saving tool into a profitable technology. Cloud Computing is considered to consist of large data centers, which offer economies of scale, cheaper computing power and, most importantly, the flexibility to pay only for what you use. IT services for individuals and organizations are hosted on the Internet and thus there is no need for local servers on their premises. The computers are located in data centers designed for optimal energy efficiency (for example, as close as possible to power plants). In addition, businesses and organizations avoid investing in and using additional equipment to cover their seasonal needs by simply using the cloud, respectively, without considering the purchase of additional equipment. Cloud technology can be expressed in various combinations of offered services and development models. In any case, this technology is evolving rapidly and is being adopted by users of all types, sizes and objects. This fact alone proves that the advantages and benefits it brings, such as flexibility, efficiency, strategic added value and pricing method, exceed any disadvantages and weak points of its use.
The conclusions of the research are presented in the next chapter.

Chapter 5: Research Conclusions

Methodological Model

As the aim of the work is to highlight the security of information systems and networks in the public sector with the use of cutting-edge technologies and to make a comparison with the current situation in the Greek public sector and abroad, the systematic literature review is chosen as the most objective method, within the framework of secondary research, to identify the cutting-edge technologies that have been adopted by organizations or are about to be implemented, as will emerge through the study of international literature. In this way, the present work aims to formulate proposals for interventions and strategies regarding the security of information systems in the Greek public administration by utilizing cutting-edge technologies.

Systematic reviews often, but not necessarily, use statistical methods, i.e. meta-analysis, to combine evidence from research in the literature to produce a single estimate of the effect. A systematic review is therefore an integrated method by nature and is able to address much broader questions than empirical studies (e.g. uncovering connections between multiple empirical findings). Indeed, systematic reviews are at the top of the "hierarchy of evidence" because they have the potential to provide the most important practical implications and implications of individual empirical studies (Siddaway, 2015).

According to Haidich (2010) meta-analyses are a subset of systematic reviews. A systematic review attempts to gather empirical evidence with predefined eligibility criteria to answer a specific research question. The key features of a systematic review are a clear statement of the set of objectives with predefined eligibility criteria for studies, an explicit, repeatable methodology, a systematic search that attempts to identify the set of studies that meet the eligibility criteria, an assessment of the validity of the findings of the included studies (e.g. through risk of bias assessment), and a systematic presentation and synthesis of the properties and findings from the studies used. Systematic reviews use methods to minimize bias, thus providing more reliable findings from which valid conclusions and recommendations can be drawn. Systematic reviews do not need to include a meta-analysis (quantification of findings and statistical analysis) as there are cases where this is not appropriate or possible (Haidish, 2010). Systematic reviews must be objective, systematic, and their conclusions must be replicable.

Based on the above, the choice of a systematic literature review is sufficiently justified, which constitutes a valid and objective scientific method within the framework of secondary research, for the extraction of valid conclusions from the synthesis and critical analysis of the existing Greek and international

literature on the security of information systems and networks in the Greek public administration with the use of cutting-edge technologies.

Purpose and Research Questions of the present study

The purpose of this doctoral thesis is to investigate the existing cutting-edge technologies in the Security of Information Systems and Networks and to adapt them to the needs of the Greek Public Sector.
The research questions posed for the above purpose are:

- To highlight the need for the use of security Information Systems in the Greek Public Sector.
- To state what are the cutting-edge technologies and current trends in terms of the security of Information Systems
- To identify what are the needs in the Greek Public Sector for the use of secure Information Systems
- To emphasize the need to interconnect the Information Systems of the Greek Public Sector
- To propose a way to implement secure interconnection networks based on the technology that exists today
- To capture the main purpose of e-government, ensuring the security, control and proper functioning of information systems and the information that circulates in them
- To highlight every action that results from the implementation of the current legislation regarding transparency in Public Administration

In the modern era, at a global level, the public administrations of countries are called upon to respond to the ever-increasing demands that are created during the administration and management of public affairs. The policies and legislations that are called upon to face this reality, try to shape and reshape the administrative structures in such a way as to make them more efficient, faster and less costly. This logic includes reform efforts such as, for example, the implementation of the New Public Management, a reform that aspired and aspires to resolve the dysfunctions of public administration by applying logic and practices that come from the private sector. According to Loukis E. et. al. (2008), the category of reform efforts also includes Electronic Governance. It is a philosophy of reforming public services by adopting and using the tools offered by technology. E-Government therefore concerns the use by the Public Administration of Information and Communication Technologies for the performance of its activities as well as for communication and daily transactions with citizens and organizations. The adoption and use of Information and Communication Technologies leads gradually but steadily to

a redesign of the organization, procedures, organizational structures, institutions and the exercise of relevant policies.

In the above context, the Greek state, realizing the important role of E-Government for the present and future of Public Administration, has taken relevant legislative initiatives in order to facilitate and promote the adoption and use of new technologies.

Consequently, digital technologies are an integral part of human daily life, both in private and public life. They determine the way in which it communicates, operates, carries out its economic and professional activities. They also have a decisive influence on Public Administration and Public Services. Digital technologies shape the way in which the activities of the Administration are carried out and the daily services offered to citizens and the private economy.

Greece unfortunately ranks last in terms of the adoption of digital technologies among all the member states of the European Union and, more generally, among the countries that make up the so-called developed world. This means that it is unable to enjoy all the benefits that digital technologies bring, such as the creation of new jobs, the enhancement of the efficiency of Public Administration, the removal of geographical and social exclusions. As is the case with any policy that is introduced for implementation, so too in the case of the adoption of cloud computing technology by Public Administration, a series of basic conditions, prerequisites and necessary characteristics are formed which determine the framework under which the relevant policy will be implemented. In other words, an “umbrella” of appropriate conditions is created, under which its implementation becomes possible. On the contrary, the absence of the appropriate framework makes it impossible, for practical reasons, to implement the policy, which ends up being an “empty letter”.

The most basic condition for the implementation of any policy is the existence of the appropriate political will. The almost absolute dependence of projects on the intentions of the political factor, whether at the level of individuals (e.g. Ministers) or at the level of institutions (e.g. ruling party), demonstrates the magnitude of this significant pathogenicity. In this context, the implementation of projects is included in frequent political circles and becomes a “tool” in the quiver of political personnel who use them as they wish as a tool to achieve their own goals. The complexity of the phenomenon is exacerbated by the implementation time of many projects, which often exceeds the “lifespan” of governments, thus placing them under the judgment of more political figures who often differ in terms of political ideology and targeting with the pre-existing situation. Thus, a project that for the previous political order may have been a “flagship” project, for the next political situation may be undesirable. Often, overcoming these issues is expressed by calling for the adoption of “national policies” in specific areas of public life that will be above political confrontations and therefore can be served by all political trends. The human factor that determines the course and implementation of various policies is not

limited to political personnel. Public Administration personnel, who staff the services and organizations, also play an important role. Both junior staff, ordinary employees, and executives at the highest levels of the hierarchy play their role in the course of execution of a project. Thus, as a collective entity with self-awareness, they express their opinion on the policies and reforms planned for the Public Administration. Through their collective bodies, they can approve or oppose a reform effort or project. The attitude they maintain in each case significantly affects the development of the relevant effort, resulting in anything from simple delays in implementation to its abandonment or cancellation.

In addition, an important factor that determines the attitude of civil servants towards various policies is their degree of familiarity with said policies. In the specific case of the adoption of cloud technologies, the level of digital literacy of civil servants plays an important role in the speed of development of the project and the degree of its assimilation. Public Administration must contribute to the improvement of the technological skills of employees through seminars and training programs.

It is worth mentioning that a restraining factor in any reform effort is the practice of transferring employees to key positions in ministries and public services. In addition to the questionable purpose and role they serve (such as the politician who appointed them, their personal agenda, the public administration), their transferable presence creates significant continuity problems in critical positions in the administration every time there is a change of government and political leaders.

In addition to the existence of the appropriate framework for the implementation of projects such as the adoption of cloud technology, the existence of standards of mainly technical content that define the uniform development and use of the technology is also important. In particular, in the case of Greece where information systems were developed for years in a fragmented and non-uniform manner, resulting in their non-interoperability, it is particularly important that new technology projects are carried out with a view to providing for this issue. Investments in equipment and software for the adoption of cloud technology should be made with the fundamental condition and prerequisite of the interoperability of the systems. To achieve the above, the Greek public administration should adopt and apply in every technology project, the standards set by the European Union.

Cloud computing is a set of infrastructures that is fully managed by a provider. From the moment an application is combined with cloud computing, the organization that uses it is released from any kind of obligation to upgrade, maintain and user licenses and by extension from additional costs. This helps organizations to focus on their subject matter seamlessly, without the fear of any downtime due to damage to certain programs and applications they use.

Browser security is an important issue in Cloud Computing since in a Cloud Computing, calculations are performed on remote servers and the client

computer (i.e. the peripheral computer) is used only to make the transfers of information (information input - information output) and to certify the commands in the Cloud.
In terms of cost, cloud computing currently offers affordable prices, on a large scale for businesses. If the economic case prevails, then we can say that nothing will prevent cloud computing from becoming a consumer good.
The advantages offered by Cloud Computing are such that over time all data will be located with one of the providers. Cloud Computing provides security and reliability, which are the most basic issues that each organization needs for its data. The computing resources offered by each provider are such that even large organizations would have difficulty obtaining them, as the risk after purchasing them would be very high. Every organization that uses Cloud Computing, in addition to the security issues and the resources offered to it, can reduce the risk of its respective application. This can be done, as there is the possibility for each application to be tested in real conditions locally before it is delivered for common exploitation.
However, beyond the positive aspects that arise, the security and especially the legal landscape regarding Cloud Computing is still fraught with uncertainty. Many concerns arise especially at the level of ensuring privacy and personal data, and by extension whether the user can control which of his personal data is retained during his browsing and use of cloud services. In the future, it is considered certain that cloud service providers will continue to find economies of scale, not only for their basic services but also to achieve security management.
Finally, regarding the future of Cloud Computing, large organizations will maintain in-house functions of a significant nature, confidentiality, privacy and absolute ownership are a matter of minor importance. For the future, the goal will be for the technologies and institutional framework surrounding Cloud services to mature and develop in order to offer new opportunities and challenges to all users.
Concluding that, cloud computing services are cutting-edge technology that has entered the everyday lives of people, organizations and the Public Sector for good. Particularly in the case of the latter, cloud technology is one of the vehicles that will bring Public Administration and Public Services on a path of redefinition in terms of their effectiveness, efficiency and speed with which they manage public affairs. Public Administration aspires and aims to overcome its sterile bureaucratic past, the inefficiency and rigidity that characterized it for decades and that had completely discredited it in the consciousness of citizens, and cloud technology can offer excellent services in this direction.
Recognizing the potential of cloud technology and the catalytic role it can play in the reform of Public Administration, the state has been taking appropriate measures and legislative initiatives over the last decade or so. Of course, a legislative text ends up being an “empty letter” if there are no appropriate

conditions and the will of all stakeholders to implement it. Unfortunately, for the Greek Public Administration, the coincidence of all the above conditions is difficult to achieve, for various reasons, which makes the adoption of cloud technology a particularly uphill road. It is necessary for the healthy forces involved to fight so that this technology does not become yet another missed opportunity for the reform of the Greek Public Administration.

According to Heeks (2005), in order to ensure transparency, public bodies should move boldly towards open data, i.e. the free availability of their public data, as in addition to enhancing transparency and consultation with citizens, they can constitute a digital raw material for enhancing the economic development of a region/country. This stems from the fact that the added value of publicly available information and knowledge consists in the ability to manage and reuse it by both the public and private sectors for the production of innovative electronic services.

The trend of open data has been gaining momentum over the last five to ten (5-10) years, with the Obama Administration's "Open Government Initiative" since 2009 as a milestone, and in particular the creation of the federal electronic portal data.gov, which contains a wealth of open data (datasets). Some countries have taken similar important steps, such as the United Kingdom. Notable is the creation of the international organization "Open Government Partnership", which was founded on September 20, 2011 by 8 important countries in the world (Brazil, United States, United Kingdom, Indonesia, Mexico, Norway, South Africa, Philippines) and within two years another fifty-seven (57) countries have joined it. The purpose of its operation is to secure specific commitments from each participating country to promote transparency, empower citizens, and combat corruption - through the use of new technologies and the systematic monitoring of actions to implement commitments by the international organization in question. In conclusion, in order to improve the current situation and achieve a faster pace of progress, a structured assessment of the progress made so far and the drawing of conclusions from failures and successes is appropriate. A favorable factor is the fact that the user side (citizens/organizations) is generally characterized by a positive attitude towards the e-government project. Current users recognize the benefits of electronic services and there is also a large portion of potential users due to the ever-increasing percentage of the population that is familiar with new technologies, which also has high expectations regarding the benefits generated from the future use of such services.

In the country's effort to adopt modern technologies and specifically in the development and operation of cloud computing infrastructures and services, it receives significant assistance and impetus from the policies and financial assistance of the European Union.

Therefore, from the above, we conclude that cloud computing is an innovative technology, through which organizations are given the opportunity to improve their business operations, serve their customers' needs faster, reduce their

costs and become more competitive. In short, it contributes to adding value to organizations that decide to adopt it. This is due to the flexibility it offers to organizations and consumers, namely the scalable provision of services that are selected each time according to the needs of each case and the facilitation of cooperation with commercial partners and customers.
However, there are still security and confidentiality issues that need to be resolved, which make cloud computing a controversial technology for a large percentage of organizations, which hesitate to adopt it due to the risks they estimate to be inherent to their business data and business secrets, which are maintained in such environments that are accessed via the Internet.
According to the research conducted by Billis (2011) each security manager can check whether the data stored in organizational networks and/or information systems that have access to the Internet are secure. Communication with the Internet, by its very nature, is two-way. Malicious users of information systems identify problems and do not hesitate to exploit them to their advantage. The exploitation techniques they develop and the time they invest in creating new ones, inflate the security problem, while they are often one step ahead of security managers in identifying vulnerabilities.
We could say with certainty that it is not possible to have absolute security and zero risk. All the defender can do is try to reduce the vulnerabilities of the system to zero. Also, an important factor is the timely updating of security systems so that the system administrator can prevent an ambitious attacker who uses the latest exploits and the most recent updates of attack tools. The tools are a very good option for continuous and regular control of an information system, but they cannot guarantee security by themselves. Every system must have a responsible, experienced, available and insightful administrator who is available to prevent any possible threat. Ultimately, the more the human factor is included, the greater the risk. Therefore, cloud computing is an important tool with the adoption of which one could say that all kinds of organizations, regardless of size and sector, can benefit overall. Two of its most important benefits are cost reduction and the flexibility it offers. On the other hand, based on the literature, it is observed that there are many challenges that need to be addressed, such as security and privacy issues, incompatibilities with the existing technological infrastructure of organizations, service interruptions, and political issues that prevent its spread at a global level. Solving problems such as the above will help in the creation of global cloud markets for the exchange of standardized services.

Concerns…

1) Disaster strategy
On the Information Society website as well as on the Information Society Gcloud website, while there is a satisfactory description of the services offered and general information about the cloud services offered, no reference

is made to the disaster strategy applied. The existence of a disaster strategy is absolutely necessary for the potential user to trust the provider and to be sure that his data and electronic activities are secured in the event of either natural or fraudulent disaster. For the Information Society cloud services, two cases arise, a) either there is no disaster strategy in place, b) or there is one and it is not posted on the relevant website. Similarly, neither on the cloud services website of the General Secretariat for Information Systems is there any mention of the existence of a disaster strategy plan.

2) Collaboration with a private provider

The lack of a disaster strategy from Gcloud raises the issue of finding an alternative way to ensure against unforeseen disasters. The obvious solution revolves around collaborating with a private provider after concluding a strict SLA. Therefore, the reasonable question arises as to why the State does not safeguard its interests by proceeding with such a collaboration.

3) Human resources

According to data from the Information Society, its human resources, which amount to sixty (60) people, are overwhelmingly composed of non-permanent civil servants. Although this seems positive at first glance, the criticality of the infrastructure hosted in its facilities and the sensitivity and seriousness of the data stored and the operations performed raise serious concerns regarding issues of security and trust. Indeed, personnel working on a service provision contract for a specific, usually short period of time, raises additional issues of concern for the security and protection of activities.

4) Technical personnel

Another interesting issue arises from the composition of the Information Society's human resources. As it appears, almost all of the technical human resources are employed under private law contracts, that is, they are non-public employees. Therefore, if private technicians and programmers are responsible for the operation of the Information Society's Gcloud, a very important argument against the cooperation of the public sector with private cloud service providers is missing. Provided that a strict SLA is agreed upon, the choice of cooperation with private providers becomes particularly attractive and advantageous.

5) Software licenses

In the traditional architecture where each service or organization of the State autonomously develops its own database and its own computer system, it also has the obligation to ensure that the equipment and software it uses has the necessary licenses. These licenses should be renewed at regular intervals in order to legally extend the possibility of using the relevant products. Due to the financial constraints of recent years, the reduction of funds and the effort

to save resources, many users have neglected their renewal, resulting in using the products without active licenses.
This fact constitutes a restraining factor for the transition of information systems to Gcloud. In particular, both the Information Society and the General Secretariat for Information Systems explicitly state on their websites that the interested party to transfer to Gcloud infrastructures should “have regulated the issues of lending applications and structural elements so that its legal operation is possible”.
Regarding the issue of licensing, an additional important issue arises. Large software solution providers such as ORACLE offer licenses for their products per computing core of the user’s equipment. This creates a problem with the transition to Gcloud because its architecture is based on the creation of virtual machines, each of which has its own virtual core. In order for the product on which the user has developed his applications to continue to be licensed, it should now be licensed not for the physical core but for all the virtual cores that have been created on the physical core. Thus, the required permits multiply and the costs for their acquisition become prohibitive.

6) Legal framework

The basic condition for the development and operation of a project is the existence of the appropriate institutional framework, that is, the legislative basis on which and based on which it is structured and operates. This condition seems to be bypassed by the Information Society, which has created Gcloud infrastructures and offers corresponding services to Public Administration bodies, without this possibility being mentioned either in its founding law or in its amendments.

7) Administrative discontinuity

The phenomenon of the existence of phenomena of administrative discontinuity in Public Administration is not rare, a fact that affects the implementation and operation of projects and reforms. In the case of the process of adopting cloud computing technologies, a typical example is the case concerning the Memorandum of Cooperation for the development and operation of Central Computing Infrastructures of the Greek State. The Memorandum was signed in 2010 and provided for a three-year duration. It also provided that its supervisory authority would be the Special Secretariat for Digital Planning, which was abolished in 2012, one year before the expiration of the Memorandum.

8) Obligation to transition

The Gcloud infrastructures of the Information Society were created in order to host the databases and information systems of the various organizations and bodies of the State. At the same time, the General Secretariat for Information Systems can play the same role. Given that Public Sector structures are not independent units that operate autonomously according to how they perceive

their mission and interests, but rather operate based on a central plan that comes from the respective political leadership, it raises reasonable questions as to why the State has not taken steps to issue a legislative provision that would require the gradual transition of all computer systems to the facilities of either the Information Society or the General Secretariat for Information Systems and the parallel prohibition of the creation of new independent information systems.

Suggestions for Future Research…

Regarding cloud computing technology and the factors that play an important role in its adoption by organizations, there are many aspects that could be the subject of study and research in the future.

Firstly, the security and confidentiality problems presented by the use of cloud computing services and the ways to address them. For this issue, research could be conducted to determine which problems are presented with the greatest frequency and to what extent. This could be done by studying services provided by well-known providers such as Amazon, Google, IBM, Yahoo, e-Bay and Microsoft, so as to propose countermeasures such as stronger data encryption algorithms, more secure licensing systems for access only by authorized users to valuable business data, and ways to recover damages in the event of service interruption or data loss.

Secondly, an interesting subject for further research are the restrictions arising from the governments of the countries and the various legislative frameworks, which create many difficulties in relation to the spread of cloud computing, the creation of a global market and the exchange of knowledge and information.

Thirdly, the selection of data and services to be transferred to cloud computing environments. That is, based on what criteria do the competent administrative executives of an organization choose which of their operational functions and which data they consider to be safer to keep within the organization's premises, and which do not pose a risk to its smooth operation and survival in the event of a leak due to the risks inherent in cloud computing environments, especially when it comes to public ones.

Finally, another suggestion for future research is to study cases of more organizations that have adopted cloud computing services, so as to collect more data in relation to the factors that influence the decisions of administrative executives on this issue. This will make it possible to draw more reliable conclusions and generalizations that will concern the business world as a whole.

Contribution of the Doctoral Thesis…

The contribution of this thesis lies in the important role that information systems play in public organizations. Their benefits concern both employees, making them more efficient and of higher quality in their work, and citizens, who are served directly and quickly by public organizations. Also, information systems tend to eliminate the enormous bureaucratic problems of the public sector. However, other steps are required to achieve efficiency to a high degree. Furthermore, continuous evaluation of information systems is required in order for them to operate effectively and bring benefits to the Public Administration. In addition to the evaluation of information systems, continuous upgrading is also required with regular training of personnel. Also, the security of information systems plays an important role. The use of cutting-edge technologies such as cloud computing is the widely used technology of today, trying to eliminate risks and ensure the level of security.

Epilogue…

In our days, it is considered imperative to change the perspective, culture and mentality of every public official who must consider the organization in which he works not as a necessary evil but as his wider family and to envision, anticipate and fight for its improvement and progress. On the other hand, public administration, knowing that every change contains and at all times entails risks, is necessary to inspire, motivate and train its human resources in taking risks and not to constitute a brake on risky initiatives by creating various entanglements in its bureaucratic gears.

Especially for the Greek public sector, the mistakes, unforeseen events and uncertainty of the past should not be treated by the public administration as unfortunate events but as a welcome and constructive historical database whose recognition, understanding and methodological collection, analysis and recall of data will lead the wider public sector to a positive trajectory and will contribute crucially to its sustainable development.

Public Administration leaders should not ignore the frequent phenomenon of resistance to change that is very widespread in the behavior and negative mood and readiness for a change in mentality of employees in the Greek public sector. This means that they must be prepared to encounter and deal with resistance and thus they should remain vigilant in achieving strategic goals.

Changes and continuous developments seem like a spinning top that is constantly spinning, no one knowing when it will stop. This perpetual continuous movement encompasses and embraces opportunities and risks that modern public administration must decipher, recognize and manage in

the best possible way, setting as its primary goal the viability of the Greek Public Sector and its sustainable development.

Cloud computing is undoubtedly a very useful tool that, if used in the right way, can have many positive effects on organizations and their operation. On the other hand, no one can also deny that it is a technology with the adoption of which an organization is automatically called upon to manage and face several problems that are likely to appear due to the risks inherent in this type of environment. What is certain, however, is that this happens with every technology used by an organization because each one has advantages and weaknesses.

What an organization may need to do in order to exploit cloud computing to its advantage and at the same time minimize the possibility of causing damages and losses that can have a serious negative impact on its reputation and operation, is to make a proper assessment of the business data and functions that will be transferred to the cloud computing environment. That is, the vital business data and functions should be stored within the organization's premises, or in private cloud environments for the management of which the organization itself or a trusted third party is responsible, and the rest for which the case of unauthorized access, loss or temporary interruption of service will not be catastrophic and will generally be dealt with easily and quickly, should be transferred to the cloud. Also, great attention should be paid to the formation of the agreement (SLA) when concluding the cooperation between an organization and its provider, in order to settle important issues such as disaster management, data loss, unauthorized access, service interruption and termination of cooperation in the event that it is determined that the services provided do not benefit the organization to the expected and desired extent.

Final Comment...

From this paper it is concluded that cloud computing technology is not just an ordinary technology. It is the type of technology that is not only consolidated and widely used but also manages to become a structural element of its sector. As such, it is expected to monopolize interest in the coming years in the field of information technologies. Its potential is demonstrated by the turnover it achieves worldwide, by the fact that IT giants such as Microsoft and Google compete hard to prevail in its provision, by the fact that institutions such as the European Union promote and promote it with a multitude of actions, by the fact that countries implement projects for its introduction into their public administrations.

In the above reality, Greece today appears to lag behind in the use of cloud computing technology compared to the countries of the developed world and

most countries of the European Union. The reasons for this are many and well-known and are repeated in every reform effort that is attempted. So if the inhibiting factors are so broad and have such deep roots, how is it possible to overturn them? The answer is as trivial as the pathologies that need to be addressed. What is required is a change of mentality from society as a whole. The logic of “I want change but I want everyone else to change except me” no longer has any effect.