Вх. № МС-БС-01-К /
27.05.2024 г.

К о н ц е п ц и я

за стратегическо управление на тема:

„Усъвършенстване на основните процеси в администрацията на Министерския съвет в контекста на електронното управление“

изготвена от

Габриела Николаева Козарева

за участие в конкурс за длъжността „главен секретар“ на Министерския съвет

София, май, 2024г.

СЪДЪРЖАНИЕ:

I. Увод

Настоящата концепция за стратегическо управление е изготвена за целите и съгласно изискванията на конкурс за заемане на длъжността „главен секретар" на Министерския съвет.

Съдържа схематично очертаване на устройството и функциите на администрацията на Министерския съвет и ролята и задълженията на главния секретар, като административен ръководител на общата и специализираната администрация.

Акцентът е поставен върху въвеждане на принципите на електронното управление, анализ на необходимите ресурси за постигането на целите, отчитане на затруднения при реализацията и формулиране на желаните резултати.

Предложени са методи за преодоляване на установените пропуски, които включват приложение на мерки от краткосрочен, средносрочен и дългосрочен характер.

Успешното реализиране на концепцията за електронното управление като водещ модел за вземане и изпълнение на решения ще повиши ефективността на държавното управление, като едновременно с това ще усили доверието към институциите, ще даде на гражданите и юридическите лица обосновано усещане за споделено упражняване на власт и несъмнено ще укрепи устоите на демократичните процеси.

Крайният резултат ще се изрази в законосъобразно, полезно, стабилно, сигурно, мотивирано, прогнозируемо и устойчиво управление.

II. Статут, структура и функции на администрацията на Министерския съвет. Процеси в администрацията на Министерския съвет

1. Администрацията на Министерския съвет – статут на администрация, осигуряваща изпълнението на решенията и задачите на Министерския съвет

Правната доктрина, чрез прилагане на функционалния подход, разглежда и възприема изпълнителната власт като едно цяло от правителство и администрация. Безспорно, висш държавен орган и естествена еманация на държавната власт е правителството, т.е. Министерският съвет. Понятията „правителство" и „Министерски съвет" се явяват синоними.

Разпоредбите на Конституцията на Република България (КРБ) – Глава пета, възпроизвеждат това разбиране, като въвеждат нормата, че правителството осъществява и координира държавното ръководство, а държавната администрация, в частност администрацията на Министерския съвет, осигурява техническото и организационно реализиране на управленските решения. В чл. 108, ал.2 от КРБ е очертана и т.н. „компетенция на компетенциите" присъща на министър-председателя – „ръководи и координира общата политика на правителството и носи отговорност за нея".

Министерският съвет е висш държавен централен орган с обща компетентност, а неговата администрация, съобразно с целите и правомощията на органа, който подпомага, следва да обслужва процесите по вземането и реализацията на политическите решения, чрез осигуряване на информация, анализи и експертиза.

2. Структура на администрацията на Министерския съвет (АМС). Роля и функции на главния секретар на Министерския съвет

В съответствие с разпоредбите на Закона за администрацията (ЗА) и в изпълнение на неговия чл. 41, Устройственият правилник на Министерският съвет и неговата администрация (УПМСНА) урежда структурата, състава и функциите на отделните звена.

Глава четвърта, раздел I от УПМСНА очертава задачите на администрацията като изрично сочи, че тя подпомага Министерския съвет при реализиране на неговите правомощия. Раздел II от същата глава урежда функциите и задълженията на главния секретар на Министерския съвет. По същество и съобразно специфичните правомощия на правителството като колективен орган, главният секретар организира, координира и контролира изпълнението на задачите от отделните звена на администрацията, осъществява взаимодействието с политическите кабинети на министър-председателя и заместник министър-председателя, осигурява взаимодействието с другите администрации, изпълнява и изрично възложените му от министър-председателя функции. Несъмнено, най-важното от определените му задължения е това по организацията, координацията и контрола на подготовката на заседанията на Министерския съвет и оформянето на приетите актове.

Чл. 63 и следващи от УПМСНА, според разпределението на функциите, разграничават администрацията на Министерския съвет на обща и специализирана. Общата администрация осигурява технически дейността на Министерския съвет и на специализираната администрация и осигурява административното обслужване на гражданите и юридическите лица. Общата администрация е разделена в четири дирекции, както следва: „Правителствена канцелария", „Бюджет и финанси", „Административно и правно обслужване и управление на собствеността" и „Информационни и комуникационни технологии".

Към на главния секретар на Министерския съвет са създадени и шест отдела на пряко подчинение: отдел „Административна и регионална координация", отдел „Човешки ресурси", отдел „Контрол по изпълнението на актовете и договорите", отдел „Правителствен протокол", отдел „Сигурност на информацията" и отдел „ПЗДНСЕИВГО". Главният секретар осъществява и контрол по администрирането на дейностите на секретариатите на съвети към Министерския съвет.

Чл. 69 и следващи от УПМСНА уреждат статута на звената от специализираната администрация. Тя е разделена в девет дирекции: „Правна", „Координация на политики и концесии", „Координация по въпросите на Европейския съюз", „Вероизповедания", „Стратегическо планиране", „Добро управление", „Модернизация на администрацията", „Правителствена информационна служба" и „Централизирано възлагане на обществени поръчки".

3. Процеси в администрацията на Министерския съвет

Процесите, които се изпълняват от звената в администрацията на Министерския съвет, следва да са съответни и да спомагат осъществяването на конкретните правомощия и задачи на правителството. Анализът недвусмислено сочи, че процесите, които са в пряка връзка и се явяват определящи за ефективното и законосъобразно изпълнение на задачите и решенията на Министерския съвет са тези, които се осъществяват и са възложени на звената от специализираната администрация. Специализираната администрация винаги е тази, която отговаря за специфичните и характерни за съответния орган правомощия и задължения. Обхватът на процесите и характеристиката на задълженията на звената от специализираната администрация на Министерския съвет се отличава от останалите специализирани административни звена по това, че нейната специализация всъщност трябва да осигурява изпълнението на задачи на орган с обща компетентност. Последното налага различен подход към изпълнението на възложеното, доста по-високо ниво на аналитичност и широк диапазон на експертизата.

Въпреки мащабността на процесите, осъществявани от администрацията на Министерския съвет, като ключови могат да се определят тези по подготовката на заседанията на Министерския съвет, изготвянето на актовете на правителството и захранването на Министерския съвет с обосновани, мотивирани и изчерпателни становища, базирани на сериозни проучвания от различните области на знанието, необходими при формулирането на управленските решения.

Възможността или пречките за реализирането на тези процеси, в контекста на електронното управление, ще бъдат разгледани, чрез анализ на отделните елементи, необходими за успешната им реализация.

III. Електронно управление – рамка, елементи, цел

Легалната дефиниция на „електронно управление" е дадена в параграф 1, т. 39 от Допълнителните разпоредби на Закона за електронно управление – „"Електронно управление" е реализиране от административните органи на правните взаимовръзки, административни процеси и услуги и на взаимодействието с потребителите, с лицата, осъществяващи публични функции, и с организациите, предоставящи обществени услуги, чрез използване на информационни и комуникационни технологии, осигуряващи по-високо ниво на ефективност на управлението".

Осъществяването на целите на държавното управление в областта на информационните и комуникационни технологии се подчинява както на императивните изисквания на действащото в страната законодателство, така и на действащото общностно право и на международните стандарти /ISO/IEC; NIST и др./.

1. Регулаторна рамка на национално и европейско ниво. Стратегически документи и нормативни решения в сферата на електронното управление и киберсигурността

Към настоящия момент, в рамките на националните политики, съобразени и отразяващи европейските и световни стандарти, действат и са в процес на прилагане няколко национални стратегически документа, които отчитат нивото на достижения и очертават глобалните цели в областта на електронното управление, реформата в публичния сектор, регистровата реформа и киберсигурността. Последните техни редакции са както следва:

- Актуализирана стратегия за развитие на електронното управление в Република България 2019 – 2025 г. /март 2021г./, ведно с приложенията към нея – 1. Актуализирана пътна карта за изпълнение на Актуализираната стратегия за развитие на електронното управление в Република България и 2. Концепция за регистрова реформа;
- Актуализирана национална стратегия за киберсигурност „Киберустойчива България" 2023 . /2021г./;
- Цифрова трансформация на България 2020- 2030;
- Архитектура на електронното управление в Република България / ДАЕУ, 2019г./ и др.

Общностното право също отделя особено внимание на регулацията на процесите в областта на информационните технологии с подчертан акцент на защитата на лични данни, спазването на минимални нива на мрежовата и информационна сигурност /хардуерни и софтуерни решения/, електронната идентификация, киберсигурността, особено в частта превенция от посегателства. На европейско ниво следва да се отбележат Директива 2019/1024 за отворените данни и повторното използване на информация от публичния сектор, Регламент 2019/881 относно ENISA и сертифицирането на киберсигурността на информационните и комуникационни технологии, Директива 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, Регламент 910/2014 относно електронната идентификация и удостоверителните услуги при електронни трансакции, Регламент 2016/679 – Общ регламент за защита на личните данни Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022г. относно мерките за високо общо ниво на киберсигурност в Съюза, и разбира се, одобрения на 13 март 2024г. Акт за изкуствения интелект на Парламента на Европейския съюз /паралелни процеси на регулация, с висок интензитет, протичат във всички държави, с водеща роля на САЩ – на 13.05.2021г. американският президент подписа Изпълнителен указ за киберсигурност, който въвежда строги изисквания към софтуерните доставчици на правителството за високи нива на киберсигурност на продуктите/.

Цитираните по-горе национални стратегически документи, служат като ориентири при изпълнението на конкретните дейности и залагат като основни, **общовалидни принципи за утвърждаването на електронното управление (e-government)**, с цел преминаване към **мобилно управление (mobile government),** еднократното събиране на данни, SOA – изграждане на архитектура, насочена към предоставянето на услуга /Service

Orientated Architecture/, изпълнение на услугите, съгласно принципа **дигитално по подразбиране** и един от водещите и също така вече нормативно скрепен принцип на комплексно административно обслужване /КАО/.

Правната рамка на електронното управление в Република България обхваща Закона за електронното управление, Закона за киберсигурност, Закона за електронния документ и електронните удостоверителни услуги, Закона за електронната идентификация, Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, Наредбата за обмена на документи в администрациите, Наредбата за удостоверенията за електронен подпис в администрациите, Наредбата за административния регистър, Правилника за прилагане на Закона за електронната идентификация, Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги и Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).

2. Принципи на електронното управление. Модели на взаимодействие

Електронното управление, като феномен, стъпва върху няколко основни принципа, които са насочени към осъществяването на дигиталната трансформация на обществото и гарантират високи нива на ефективност, демократичност и устойчивост в сферата на държавното управление.

Стратегическият документ „Актуализираната стратегия за развитие на електронно управление в Република България 2019 – 2025г." дефинира основните елементи на електронното управление в държавната администрация: правна рамка; оперативна съвместимост; електронна идентификация; работни процеси; информационни ресурси (в това число споделени ресурси на електронното управление) и тяхното развитие, електронни услуги; регистри и данни; мрежова и информационна сигурност; киберсигурност.

Разгръщането на потенциала на данните, а оттам цифровата трансформация, ще позволи използването на интелигентни технологии, с възможност за анализ и вземане на решения чрез обработка на големите данни (big data analysis). Последното е особено приложимо към държавните институции, като такива, акумулиращи огромни обеми от данни. Ефективното генериране, обработване, съхраняване и повторно използване на натрупания ресурс ще повиши качеството на публичната услуга (включително на държавното управление). Освен прекия ефект от вземането на решения на база на обработката на значими количества данни, предоставянето на достъп на гражданите, чрез порталите за отворени данни, ще мултиплицира ползата, като засили усещането за демократичност и участие на гражданското общество в прекия процес по взимане на решенията и определяне на стратегическите цели.

Практиката е установила три модела на взаимодействие при реализирането на дейностите по електронното управление: администрация – граждани; администрация – бизнес и администрация – администрация.

В публичното пространство по-голямо внимание и значение се отдава на първите два модела на комуникация, вероятно защото са по-видими. Всъщност, за въвеждане на ефективно електронно управление е необходимо да се въведат и експлоатират в максимална степен възможностите на информационните технологии и в третия модел – комуникацията администрация – администрация или т.н. вътрешен обмен.

За да отговори на очакванията, АМС следва да предприеме мащабни и интензивни действия по дигитализиране на информационните си масиви, които дигитализирани и приведени в машинно четим формат, да се съхраняват в технологично съвместими информационни системи (ИС). Това ще позволи автоматизиране на голяма част от процесите, ще гарантира по-високи нива на конфиденциалност и интегритет на ползваната и предоставяна информация и разбира се, ще съкрати сроковете на изпълнение на административните задачи.

В настоящото изложение ще бъдат разгледани тези от посочените по-горе основни елементи на електронното управление, които представляват ключови предизвикателства пред оптималното реализиране на последното в рамките на АМС и върху които АМС и ръководството и могат да упражняват влияние.

IV. Предизвикателства пред АМС при въвеждане на елементите на електронното управление

1. Ресурсна обезпеченост – хардуер, софтуер, кадри

Нивото на въвеждането и употребата на информационни и комуникационни технологии (ИКТ) в АМС не може да се определи като твърде високо, въпреки това по-съществения проблем е видимият пропуск по отношение на мерките за защита – мрежова и информационна, киберсигурност и дори киберхигиена. Наблюдава се липса на квалифицирани кадри, които да могат да внедрят или да ползват ефективно наличните хардуерни и софтуерни решения, съответно да подходят аналитично и да предложат възможни решения за оптимизиране. Като първа стъпка, АМС трябва да изгради една работеща, ефективна и сигурна архитектура на информационните си системи, като цяло, а след това, в кратки срокове да я надгради по начин, който да посреща нуждите и изискванията за висока производителност и киберустойчивост.

Паралелно трябва да се въведат мерки за защита на всяко едно от нивата – физическа, логическа и технологична защита. Провеждане на обучения за повишаване на квалификацията на служители – както от специализираната ИКТ дирекция, така и като цяло, също е задължително условие, тъй като съгласно световната статистика, огромният процент от пробиви в сигурността се дължи на човешки грешки.

Анализът на състоянието на ИКТ структурата на АМС сочи наличие на системни грешки и липса на последователност и дългосрочно планиране при вземането на решения, довело до „съжителстване" на разнообразни технологични решения, несходими една с друга информационни системи, многообразие от производители и доставчици, употреба на нелицензирани продукти или до нерегулярно снабдяване с необходимите лицензи, съхраняване на сензитивни и критични данни върху носители, които нямат възможност за гаранционна поддръжка, липса на резервни копия и много други.

В последните години, законодателят направи задължителни за администрациите изискванията за минимални нива на мрежовата и информационната сигурност, реда и начините за разработване и възлагане изграждането на информационни системи (ИС), както и на всички проекти с ИКТ насоченост, въведе правила за собствеността, вида и съхранението на сорс-кодовете и изходните кодове, за хранилищата, контрола на версиите и ред други. По отношение на АМС огромната част от тези изисквания са все още неизпълнени, а по отношение на някои от експлоатираните ресурси и неизпълними (АМС ползва продукт, който е собственост на юридическо лице - разработчик, което вече не съществува).

Тези констатации еднозначно очертават краткосрочните задачи пред АМС – да опише и анализира състоянието на информационните си ресурси, да определи ИКТ нуждите си, да формулира устойчиви и работещи решения, като още в процеса на анализ и дизайн на архитектурата на ИС заложи минималните или по-високи изисквания за мрежова и информационна сигурност, възможност за сходимост с ИС на други администрации /органи/, залагане на функционалности по структуриране и обработване на масиви от данни и представянето им в машинночетим формат на заинтересованите страни. В плана за действие задължително следва да се включат и въпросите относно защитата от кибератаки, изграждане на системи за сигурно съхранение и обработка на данни, осигуряването на резервираност на данните и процесите, поддържане на работоспособността и отказоустойчивостта на системите и избягване на риска от инциденти.

Както всеки субект на публично финансиране, така и АМС като първостепенен разпоредител с бюджет (ПРБ), прави прецизна преценка на бюджетните си възможности. Реализирането на етапи от гореописаното, освен чрез преки инвестиции в собствени ресурси, може да се осъществи и чрез модерни технологични решения като облачните услуги, във всички познати варианти. Към настоящия момент АМС покрива много малък процент от ИКТ нуждите си чрез използване на пространство на Държавния хибриден частен облак (ДХЧО). Използването на облачни технологии е решение и при недостиг на персонал или при недостатъчна квалификация на част от

него, като гарантира универсален достъп, бърза еластичност, самообслужване по заявка, обединяване на ресурсите и мащабируемост на услугата.

2. Киберсигурност

Като отделен и базов приоритет при изграждане на устоите на електронното управление трябва да се обособят дейностите свързани с киберсигурността. Важността на този приоритет се определя от два фактора, а именно – изключително бързото нарастване на броя и вида на киберпрестъпленията в световен мащаб, в комбинация с ниското общо ниво на познания по отношение на мерките за киберсигурност у ползвателите на ИКТ услуги, в частност служителите в АМС. Мерките за мрежова и информационна сигурност в АМС не са в съответствие с тези, възприети като стандарт на европейско и световно ниво /през 2022 година в сила влезе и новата директива за мрежова и информационна сигурност – NIS 2 – Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерките за високо общо ниво на киберсигурност в Съюза/, а дори и формално въведените не се прилагат ефективно.

Анализ на Съвета на Европейския съюз сочи като най-често срещани следните пет вида атаки: малуер, уеб-базирани атаки, фишинг, атаки през уеб-базирани приложения и спам. Информационни системи, изградени на уеб-базирани услуги и приложения, в комбинация с ниско ниво на киберхигиена отварят широко вратата за инциденти със сигурността на системите и интегритета и конфиденциалността на данните. Задължително е спазването на водещите принципи на **Триадата на Киберсигурността** – CIA Triad– Confidentiality, Integrity, Availability – **Конфиденциалност, Интегритет, Достъпност**. Всеки един от тези елементи трябва да бъде гарантиран, както по отношение на мрежите, така и по отношение на информацията. Това е особено важно за системите и информацията/данните генерирани и ползвани в държавната администрация, поради високия обществен интерес, който обслужват и поради значимите щети, които могат да настъпят при реализиране на рискови събития и киберинциденти.

Следващ етап при изграждането на система за киберсигурност е въвеждането на метрики за оценка на мерките по киберзащита, защото няма архитектура или защита, която да е напълно непробиваема. Абсолютна превенция не е възможна, поради което следва да се въведе като императив регулярното провеждане на риск анализ и своевременно актуализиране на мерките за защита на физическо, логическо и технологично ниво.

3. Данните, като основа на цифровата трансформация

Електронното управление е политика, базирана на данни. Данните, а оттам и информацията, се категоризират като най-ценния ресурс в настоящата информационна ера. Всяка ера се характеризира с различни базисни ресурси – за аграрната – земята, за индустриалната – капитала, за информационната – знанията, уменията и достъпът до технологии. Ефективното развитие на даден процес зависи от ефективното управление на движещия ресурс – знанията, т.е. управление на знанията (на данните).

Данните могат да се съхраняват в структуриран или неструктуриран вид. За да служат ефикасно, е важно данните, съответно информацията, да бъдат формализирани и документирани. Информацията следва да се идентифицира и опише – заглавие, дата, автор, референтен номер, да се определи форматът – език, версия на софтуера, средата – хартиен или цифров носител. Създават се правила за достъп и разпространение на данните, контрол върху промените, правата за задържане и унищожаване.

Управлението на данните в една организация влияе пряко и е определящо за други ключови процеси – управлението на информацията, управлението на човешките ресурси и управлението на риска.

V. Предложения за практическо разрешаване на дефинираните проблеми пред ефективното въвеждане на електронно управление. Конкретни примери

1. Въвеждане на мерки и процеси, съгласно водещи стандарти. Сертифициране

Описаните затруднения, по отношение на мрежовата и информационната сигурност и киберсигурността от една страна и по отношение набирането, създаването, обработването, съхранението, предаването, архивирането и унищожаването на данните могат да бъдат преодолени чрез въвеждането на процесите, правилата и моделите заложени в ISO 27001:2022 - "Информационна сигурност, киберсигурност и защита на поверителността – системи за управление на информационната сигурност" и ISO 30401:2018 – „Система за управление на знанията".

Наредбата за минималните изисквания за мрежова и информационна сигурност, в сила от 26.07.2019г., превръща в правна норма изискванията на **ISO 27001:2017**. Ревизираният текст на посочения стандарт въвежда и допълнителни изисквания, но доколкото базовите елементи са вече част от действащия правов ред, в настоящото изложение няма да се спирам в детайли на него.

По-различно е положението с приложението на **ISO 30401:2018** – „Система за управление на знанията" (стандартът има две изменения – от 2022 и 2024 година, но е все още актуален под тази номенклатура). В действащото в страната законодателство има един единствен нормативен акт – Наредба № 69 от 16 май 2006г. за изискванията за добрата производствена практика, при производството на ветеринарномедицински продукти и активни субстанции, който ползва понятието, като в своя § 1 дава следното определение: „Управление на знанията е систематичен подход за придобиване, анализиране, съхраняване и разпространяване на информация".

Както беше посочено, днес, всички процеси в обществото се развиват и са обусловени от характеристиките на четвъртата индустриална епоха, чиито ключов ресурс и условие за просперитет са данните, информацията и формираното на тяхна база знание. Все по-често, предимно или напълно, информацията се създава, управлява и използва в изцяло електронна среда.

Знанието се дефинира като базисен актив на структурата/организацията (администрацията, в дадения случай), тъй като позволява вземането на „правилни" решения, създава устойчивост и адаптивност и се превръща в продукт само по себе си.

Организациите не следва да разчитат на спонтанното и случайно добиване и разпространение на знанията, а трябва целенасочено да създават, консолидират и прилагат повторно вече наученото. Съхраняването на знанието е важно, тъй като то, поради характеристиката си на нематериален актив, може да бъде погубено, включително поради напускане на служители. Знанието е актив, който трябва да бъде управляван като всеки друг актив на администрацията.

Системата за управление на знанията е част от общата система на управление, която представлява въвеждането на политики, правила и цели, разпределение на отговорностите по осъществяване на операциите, посредством което се минимизира рискът от липса и загуба на информация. Рискът по отношение на знанието може да се прояви като неяснота относно състоянието, непълнота на информацията, липса на познание за определено събитие, загуба на придобито преди знание или използване на съхранено знание, което вече не е релевантно и е следвало да бъде унищожено.

При въвеждане на система за управление на знанията, администрацията трябва да детерминира сферите на познание, нейните домейни на знания и веднъж формулирани, те следва да бъдат отразени по

формален начин и направени достъпни за всички заинтересовани. За да бъде ефективно предоставянето на знанието, то трябва да бъде кодифицирано и документирано (включително при предаване или заемане на позиция/пост). За да се улесни достъпът и да се осигури навременност, се предприемат действия като класифициране, въвеждане на таксономия, етикиране, определяне на номенклатури.

Много важен елемент от системата е източникът на управление на знанието. В стандарта той е наречен Chief knowledge officer – Директор по управление на знанието. В стратегическия документ „Архитектура на електронното управление – ДАЕУ, 2019г." е уредена фигурата на „Главен информационен мениджър", с какъвто служител следва да разполага всеки първостепенен разпоредител с бюджет. Изискването е, тази постоянна длъжност да е на пряко подчинение на ръководителя на административния орган и да отговаря и за второстепенните и от по-ниска степен разпоредители с бюджет. Основната функция на главния информационен мениджър е да определя единна политика в областта на електронното управление. Двете позиции са видно еквивалентни и по отношение на АМС, намирам, че тази функция следва да се поеме от главния секретар.

Общо решение на въпросите относно мрежовата и информационна сигурност и киберсигурността, както и по отношение на изграждането на софтуерни модели за управление на знанието (данните и масивите от информация) може да се потърси, чрез включването на АМС към списъка от администрации, които възлагат всички дейности по системна интеграция на националния системен интегратор. Решението за създаването на такова звено беше взето през 2019г. с измененията в Закона за електронното управление. Централизираното менажиране на процесите от обхвата на системната интеграция гарантира на органа - възложител единен подход, намаляване на необходимия ресурс – финансов и човешки и устойчивост на процесите по надграждане и поддръжка по време на и след гаранционния период.

В случай на въвеждане на описаните по-горе правила и процеси, може да се пристъпи и към сертифициране по посочените международни стандарти.

2. Въвеждане на система от вътрешни правила

Общо приложим принцип е, че процеси се регулират и менажират по-лесно, ако за тях съществуват писани правила, доведени до знанието на лицата, които следва да ги прилагат. Към настоящия момент в АМС се наблюдава отчетлива липса на регулации на вътрешните процеси, свързани с електронното управление, а материите, които са уредени с писани правила често са отдавна неприложими (например правилата за документооборот са базирани на система, която е премахната преди повече от година).

Като начален пакет от правила, инструкции или политики, следва да се въведат, или актуализират, следните:

1. Вътрешни правила за документооборот – електронни документи.
2. Политика за управление на служебните електронни пощи.
3. Правила за създаване и актуализиране на Риск-регистър. Стратегия за управление на риска. План за действия при инцидент.
4. Регистър на информационните ресурси.
5. Правила за работа в електронна среда – принцип „необходимост да се знае", принцип „минимум привилегии".
6. Правила за достъп и работа в Internet.
7. Политика за паролите.
8. Регистър на вътрешните правила и политики.

Изброяването е неизчерпателно.

3. Въвеждане на практика по приложение на КЕП

Нормата на чл. 25, т.2 от Регламент 910/2014 (ЕС) и ЗЕДЕУУ уреждат ex lege правната сила на квалифицирания електронен подпис (КЕП) като го приравняват на саморъчния подпис.

Регламентът дава възможност на страните - членки да определят чрез вътрешното си законодателство правната сила на обикновения и усъвършенствания електронен подпис, но спрямо квалифицирания електронен подпис еднозначно и категорично се постановява, че той е със силата на саморъчен подпис – т.е. ако законодателството въвежда изискване за полагане на саморъчен подпис за валидността на документ, това изискване ще е спазено, ако съставеният електронен документ е подписан с квалифициран електронен подпис.

В УПМСНА има изрични текстове, които сочат, че отделни действия могат да бъдат извършвани по електронен път, съответно да се полагат квалифицирани електронни подписи. Този подход при създаването на нормите изглежда следва да покаже, че прилагането на КЕП трябва да се възприема като изключение. Склонна съм да допусна, нормотворецът не е имал това предвид, още повече, че с подзаконов нормативен акт не може да се дерогира Регламент, както и акт от националното законодателство от по-висш порядък.

Важно практическо приложение би имало изричното включване в текстовете на УПМСНА на разпоредба относно начина на полагане на подписи при условията на чл. 7, ал.3 – процедурата по неприсъствено приемане на акт от Министерския съвет. Посоченият ред се прилага в изключителни случаи – дали поради необходимост от неотложно вземане на решение или поради невъзможност всички членове на Министерския съвет да се окажат едновременно на едно и също място, но поради не до край изчистената концепция за полагане на КЕП, всъщност неприсъственото приемане на акт се превръща в итеративно присъствено – всеки от членовете на правителството трябва да се окаже във физически досег с акта и да положи саморъчен подпис.

Отново следва да се подчертае, че направеното предложение за подписване на актове и други официални волеизявления, не изисква промяна в действащото в страната законодателство. Напротив – ще доведе до по-пълно и ефективно прилагане на действаща правна норма на националното и Общностното право.

По същият начин могат да се уредят и хипотезите при полагане на подпис върху доклад на вносител, финансова обосновка и т.н.

4. Създаване на публично или служебно достъпни хранилища за данни, с възможност за структурирано търсене по ключова дума или дефинирана област на знанието или правна норма

Освен налична, информацията трябва да бъде и достъпна. За да се осигури навременност и пълнота на достъпа до информация за по-широк кръг ползватели – служители на АМС е разумно да се създадат хранилища за данни, структурирани по различни критерии, в зависимост от материята, заинтересованите страни, целта и т.н. Достъпът до определени масиви може да е и публичен, може да е за служебно ползване или само за определен кръг служители.

Хранилище за данни, в най-общ смисъл, представлява и споделена електронна папка, с всички файлове, по които работят служителите в едно звено на администрацията. Чрез споделения достъп се ограничават случаите, в които определена задача може да се изпълни само от определен служител, защото останалите нямат достъп до конкретни данни.

Подобни хранилища за данни ще се окажат полезни в случаите, когато персоналният състав на звено или орган, например консултативните съвети към Министерският съвет, се променя с всяка смяна на политическото ръководство и всички налични към даден момент документи престават да бъдат достъпни, тъй като остават притежание само на конкретни лица. Към настоящия момент съществуват 51 консултативни съвета и само няколко от тях имат електронна страница. Важните функции, с които са натоварени изискват изграждането на по-устойчива институционална памет.

VI. Заключение

Чрез натрупания от мен опит, като ръководител на една от администрациите, лидер в процеса по въвеждане на електронното управление, и на база на практическите си наблюдения и оперативна информация за начина, по който протичат процесите по осъществяване на дейностите по дигитализация, намирам, че мога да допринеса за оптимизиране на процесите по въвеждане и усъвършенстване на електронното управление в АМС.

Като пряк участник в изграждането и надграждането, възложител и собственик на ИС, мога да предложа работещи решения и ефективно да координирам изпълнението. Познавам тесните места в процеса по реализация на дейностите, разрешавала съм конфликтни ситуация в процеса на работа, в процеса на определяне на ролите и отговорностите на участниците, в търсенето на причините за възникнали затруднения и знам, какви могат да бъдат източниците на риск за пълноценното и ефективно реализиране на планираното. Често срещан проблем при възлагането и изграждането на ИС или техни функционалности е невъзможността на администрацията/административния орган да формулира целите си и да предостави изчерпателна, навременна и адекватна информация при планирането на бъдещите дейности. Погрешното или непълно планиране обичайно води и до незадоволителен резултат.

След етапа на планирането, следва етапът на изпълнението, в който е задължително административният орган да е пряко и постоянно ангажиран. Ангажираността следва да се изразява в регулярни срещи между екипите на възложителя и изпълнителя, провеждане на тестови изпитвания, проиграване на сценарий, търсене на мнението на произволно избрани служители с ограничен или никакъв опит с процесния продукт, като по този начин се гарантира приложимостта му спрямо всеки потенциален потребител.

Вземането на правилни управленски решения изисква познаване на процесите, преценяване на необходимите ресурси – финансови, времеви и човешки, оценка на риска и планиране на реакция при отклонение от очакваното.

София, май, 2024г.

ИЗТОЧНИЦИ:

1. Актуализирана стратегия за развитие на електронното управление в Република България 2019 – 2025. г /март 2021г./, ведно с приложенията към нея – 1.Актуализирана пътна карта за изпълнение на Актуализираната стратегия за развитие на електронното управление в Република България и 2. Концепция за регистрова реформа, https://e-gov.bg/wps/portal/agency/strategies-policies/e-management/strategic-documents.
2. Актуализирана национална стратегия за киберсигурност „Киберустойчива България" 2023 . /2021г./; https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=5878.
3. Акт за изкуствения интелект на Парламента на Европейския съюз от 13 март 2024г. (Предложение за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на съюза, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52021PC0206).
4. Архитектура на електронното управление в Република България, Одобрена от председателя на Държавна агенция „Електронно управление" със Заповед № ДАЕУ-5040-11.04.2019 г.,
5. https://www2.e-gov.bg/.
6. Върбанова, Г., Правен режим на електронните документи, изд."Данграфик", ISBN 978-619-7530-07-0, 2020г., Варна.
7. Георгиев, В., Основи на киберсигурността, София, изд."Авангард Прима", ISBN 978-619-239-212-3, 2019;
8. Гурова, Е., А. Антонова, Р. Николов (ред.), 2012, Управление на знания, Булвест 2000, София.
9. Гурова, Е., Дулев, П., Йотовска, К.,2013, Управление на знанията – същност, основни понятия, процеси и технологии, Проект BG05PO0014.3.04-0058, ОПРЧР.
10. Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016L1148.
11. Директива (ЕС) 2019/1024 на Европейския парламент и на Съвета от 20 юни 2019 година относно отворените данни и повторното използване на информацията от обществения сектор, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32019L1024.
12. Друмева, Е., 2018, Конституционно право, Пето допълнено и преработено издание, изд. „Сиела", София.
13. Европейска Сметна палата, 2019, Предизвикателствата пред ефективното прилагане на политиката за киберсигурност в ЕС, Информационно-аналитичен документ, http:// eca.europa.eu.
14. Закон за администрацията, Обн. ДВ.бр.130 от 5 ноември 1998г.
15. Закон за държавния служител, Обн. ДВ. Бр.67 от 27 юли 1999г.
16. Закон за електронната идентификация, Обн. ДВ № 38 от 20 май 2016г.
17. Закон за електронния документ и електронните удостоверителни услуги, обн. ДВ № 34 от 6 април 2001г.
18. Закон за електронното управление, Обн. ДВ № 46 от 12 юни 2007г.
19. Закон за киберсигурност, приет от 44-то Народно събрание на 31 октомври 2018 г., обнародван в Държавен вестник, брой 94, от дата 13.11.2018, посл. изм. ДВ 15 от 29 март 2022г.
20. Калчев, К., Измерване на параметрите в системите за киберсигурност, ВА, 2018.
21. Калчев, К., Цветков К., Киберсигурност, ВА, София, 2018.
22. Конституция на Република България, (Обн., ДВ, бр. 56 от 13.07.1991 г., в сила от 13.07.1991 г., изм. и доп., бр. 85 от 26.09.2003 г., изм. и доп., бр.18 от 25.02.2005 г., изм. и доп., бр. 27 от 31.03.2006 г., бр.78 от 26.09.2006 г. - Решение № 7 на Конституционния съд от 2006 г., изм. и доп. бр. 12 от 6.02.2007 г., изм.

и доп. бр.100 от 18 .12.2015 г, изм. и доп. бр. 106 от 22.12.2023 г.).
23. Наредба за административния регистър, Обн. ДВ № 8 от 29 януари 2016г.
24. Наредба за минималните изисквания за мрежова и информационна сигурност, в сила от 26.07.2019 г., приета с ПМС № 186 от 19.07.2019 г., Обн. ДВ № 59 от 26 юли 2019г.
25. Наредба за обмена на документи в администрациите, Обн. ДВ № 48 от 23 май 2008г.
26. Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги, Обн. ДВ № 5 от 17 януари 2017г.
27. Наредба за удостоверенията за електронен подпис в администрациите, Обн. ДВ № 48 от 23 май 2008г.
28. Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО и актовете към него.
29. Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността), https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32019R0881.
30. Устройствен правилник на Министерския съвет и неговата администрация, Обн. ДВ. бр.78 от 2 Октомври 2009г., посл. изменение от изм. ДВ. бр.37 от 26 Април 2024г.
31. Цифрова трансформация на България 2020-2030, https://www.mtc.government.bg/sites/default/files/cifrova_transformaciya_na_bulgariya_za_perioda_2020-2030.pdf.
32. ISO 30401:2018 – Knowledge management systems- Requirements, International Organization for Standardization, https://www.iso.org/standard/68683.html.