Концепция за развитие на електронното управление и за осигуряване на приемственост и устойчивост на държавната политика в тази сфера

Красимир Симонски
Председател на Държавна агенция „Електронно управление“

Времевият обхват на тази концепция надхвърля текущия ми мандат като Председател на Държавна агенция „Електронно управление“ (ДАЕУ), но тя ще бъде принципната основа за моите решения и действия през оставащите месеци на мандата.

Съгласно Закона за електронно управление, функциите на Председателя на ДАЕУ са дадени в 23 отделни точки само в чл.7в, а разписани в конкретни задължения, включени в останалите текстове на закона както и тези в други релевантни закони и подзаконови актове, те надхвърлят 100. Тези задължения ще изпълнявам на принципна основа включваща водещите принципи на електронното управление както са посочени в Талинската декларация и заложени в Закона за електронно управление и принципите в киберсигурността потвърдени в добри практики на държави-членки на Европейския съюз и водещи държави като САЩ, Израел и др. както и много други принципи, които съм изградил и припознал в своя над 30 г. професионален опит.

Като Председател на ДАЕУ, ще се фокусирам върху следните приоритети:

1. **Електронно управление базирано на данни.**

Разбирайки, че **данните са основен капитал** на държавното управление, заедно със съмишленици и партньори като Световната банка, ИКТ бизнеса, научни деятели и др. ще опитам да дефинираме и следваме Рамка за управление на данните (Data Management Framework), която да постави и основите на оперативната съвместимост. Тъй като това е пряко свързано и с провеждането на Регистровата реформа, ще следвам координираща и настоятелна политика в това направление, като ще се придържам към европейската политика и препоръки за оперативна съвместимост, включително **европейската рамката за оперативна съвместимост** с нейните 12 принципа и концептуален модел. Това ще обезпечи както трансгранична оперативна съвместимост така и обмена на данни и услуги в рамките на Европейския съюз.

Задължителен принцип в рамките на този приоритет ще е изграждането на **среда ориентирана към потребителите** – гражданите и бизнеса, както и прозрачност в дейността на институциите по отношение на вътрешните административни услуги. Основен акцент ще бъде оптимизацията на **потребителските интерфейси**, търсейки обратна връзка от потребителите за подобряването им на база споделен опит при ползването им.

Като **индикатори за успех** ще ползвам индекса DESI и eGovernment Benchmark докладите на Европейската комисия, както и индикаторите на Световната банка за електронно управление.

2. **Национална екосистема за киберсигурност**

Тази екосистема ще се състои от 5 слоя, които да противостоят като верига от втвърдяващи се защитни валове пред нарушители, кибер престъпници и терористи в българското киберпространство, затруднявайки до невъзможност техните злонамерени действия. Те са както следва:

- **Национално ниво,** което да включва Интегрирана национална система за киберсигурност. Тя трябва да обхване и интегрира компетентните организации и техните системи и центрове за киберсигурност на национално ниво. Тя трябва да позволява мониторинг на националното киберпространство в реално време с цел своевременно разпознаване и реакция при масирани кибератаки с цел предотвратяване на инциденти със значително въздействие и киберкризи както и управление по време на такива.
- **Секторно ниво**, което ще включва налагане и подпомагане на **секторните политики** за превенция на риска от кибер инциденти в секторите определени в Закона за киберсигурност - енергетика, транспорт, финансови пазари, банки и др.
- **Организационно ниво**, на което ще се подпомага развитието на капацитет и способности на отделните организации (институции, компании, и др.) за киберзащита, най-вече на стратегическите обекти и операторите на критични инфраструктури. Ще продължи налагането на изисквания (минимални но най-вече съответстващи на рисковете), към всички публични институции и организации попадащи в обхвата на Закона за киберсигурност и предстоящата нова Директива за мрежова и информационна сигурност;
- **Потребителско ниво**, където целта е повишаване нивото на кибер хигиена на индивидуалните потребители чрез кампании за превенции и информираност на гражданите, както и въвеждането на централизирани мониторингови услуги за индивидуална киберзащита от разстояние.
- **Международно ниво,** цел на което е интегриране в европейската екосистема за киберсигурност на техническо, оперативно и политическо ниво.

Ще настоявам за припознаването на киберсигурността като паралелен приоритет навсякъде, където е установена зависимост от ИКТ за основните функции на организациите и правата на потребителите, както и за канализиране на финансирането му на проектен и бюджетен принцип.

3. Цифрова трансформация на държавното управление

Електронното управление стъпва на основите на **електронното правителство**, тъй като без дигитализация на институциите е невъзможно да се следват принципите на електронното управление. Ще бъдат подкрепени всички усилия за постигане на цифрова трансформация на бизнес процесите и организацията на отделните институции в страната.

Част от подхода ще бъде **централизация** и споделяне на облачни ресурси в частта инфраструктура, което да облекчи ниско-бюджетните администрации предоставяйки им високо-качествени инфраструктурни услуги и високоскоростен защитен достъп до тях. Услугите на облака на електронното управление (известен като Държавен хибриден частен облак - ДХЧО) ще се разширяват и налагат като алтернатива на ведомствените мини центрове за данни, които са с висока стойност на поддръжка, ефективност и защита, ако въобще е предвидена такава.

В същото време, облачната организация и инфраструктура, включително комуникационна, ще се оптимизира да предлага **интелигентно разпределение** на информацията и обработката ѝ позволявайки от централизирано съхранение и обработка, тя да достигне до ниво институция и индивидуален потребител с гарантирана киберзащита и прозрачност на услугата. Ще налагам технологиите на изкуствения интелект и големите обеми данни, които ще могат да се приложат и поддържат на централно ниво, но да се ползват на потребителско ниво разпределено по места.

Чрез **баланс между централизация и разпределено потребление** трябва да се освободят административните органи от несвойствени за тяхната дейност високотехнологични ИКТ процеси, при което те ще могат да се фокусират тясно в техните зони на компетентност възползвайки се от цялата мощ на върховите технологии за интелигентна обработка и анализ, както и на оптимизация на вътрешноведомствените си процеси.

Ще работя с всички институции за преодоляване на silo- ефекта, т.е. затварянето им в собствени ИКТ империи, за **да преодолеем фрагментацията** в електронното управление и да се отвори пътя за пълното интегриране и постигане на оперативна съвместимост следвайки регистрово ориентирания йерархичен подход.

Регистровата реформа няма алтернатива в това отношение и е неизбежна под диктата на информационните технологии. Тя трябва да бъде ускорена с подкрепа от най-висока позиция, включително и с контролните функции, които са вменени на Агенцията по Закона за електронно управление и Закона за киберсигурност. Те ще бъдат прилагани без изключения с цялата си строгост, ако е необходимо.

4. Добро дигитално управление (Good Digital Governance)

Електронното управление, което бих желал да бъде изградено в България, трябва да получи **доверието на гражданите и бизнеса**. Това може да стане при следване принципите на „Доброто дигитално управление“, което включва цифрово приобщаване, отворено и прозрачно управление ориентирано към гражданите, електронната демокрация, и други подобни принципи.

Трябва да бъдат установени ясно **ролите и отговорностите** на различните играчи в една организация – от ръководителя през главния информационен мениджър до всички крайни потребители. Ще изискваме налагането на дисциплината на дигиталното управление в организациите, което изисква да се трансформират голяма част от бизнес процесите им като ще им помагаме в адресиране на основните предизвикателства с инструкции и препоръки, но и ще изискваме спазване на принципите на електронното управление.

Ще поддържам налагането на ролята на **Главен информационен мениджър** (Chief Information Officer), както и на **Главен мениджър по информационна сигурност** (Chief Information Security Officer) във всяка институция, чрез който да налагаме политиката за Добро дигитално управление на експертно и в същото време достатъчно високо ръководно ниво. Ще осигуряваме обучение при необходимост и инструкции включително как да се оценява правилно риска от опериране във виртуална среда.

Ще се опитам да наложа и въвеждането на индикатори за успех в това направление, прилагайки творчески подбрана **селекция от индикатори** от европейски и световни индикатори, включително оптимално съотношение качество срещу цена (Value for Money).

5. Преминаване към мобилни технологии

Ще считам за огромно постижение създаването и налагането на **единно мобилно приложение** за достъп до електронните административни услуги. Почти всички потенциални потребители на електронното управление ползват мобилен достъп до информация и услуги, но електронните административни услуги изостават значително в задоволяването на това търсене.

Бизнесът има вече достатъчен опит в предлагането на успешни мобилни решения. Съответно, с отварянето на повече данни и следвайки последователна политика за „**отворени данни**“, ще се даде възможност за създаването на ефективни и иновативни мобилни приложения за гражданите и бизнеса. Вече има такива мобилни решения за електронна идентификация, които вече са припознати до известна степен за достъп до електронни услуги от държавата като ще гарантираме тяхната достоверност и ползване със строг държавен контрол за да се постигне доверие и пълноценно ползване от гражданите.

6. Инвестиции в човешки ресурс

Един от основните проблеми за електронното управление е намирането и задържането на **ИКТ експерти** в държавната администрация на фона на техния дефицит в страната. Предизвикателства, пред които е и ще бъде изправена Агенцията, изискват високотехнологични познания, умения и компетентности в различните информационни технологии като умения за програмиране, администриране на ИКТ системи и среди, киберсигурност, управление на бази данни, и др. Дефицитът за такива кадри обикновено се решава с високи възнаграждения, поради което държавната администрация не е особено популярна за тях. Това изисква конкурентен подход от страна на Агенцията за мотивиране и задържане на такива кадри, както и съответната гъвкава организация на проектен принцип.

Ще се опитам да изградя **ядро от водещи специалисти**, което да може да ръководи разширени проектни екипи от добавени външни или временно наети експерти съгласно спецификата на проектните дейности и задачи, които трябва да се изпълняват.

Необходима е създаването на външна **оперативна структура** под контрола на Агенцията за опериране на ключовите информационни системи в продукционен режим, както и за развитие и поддържане на интеграционната среда на електронното управление. Това може да стане под формата на държавно предприятие или друга подходяща структура под оперативния контрол на Агенцията и в изпълнение на нейната мисия.

Стремежът ми ще бъде освен да се изгради ядро от специалисти, то също така да се допълва от временно наети експерти на проектен принцип, които да осигуряват надеждното функциониране и **системна интеграция на, и към, ключовите информационни системи** на електронното управление. Те ще подпомагат интегрирането на информационните системи на останалите публични институции, които ще се разработват на конкурентен принцип, както и интегрирането на други бизнес системи.

7. Инвестиции в споделените информационни ресурси на електронното управление

Ще продължи **инвестицията в централизирана инфраструктура** на електронното управление или т.н. споделени информационни ресурси на електронното управление**. Държавният хибриден частен облак** ще се развива на етапи, които ще се определят от търсенето на неговите услуги на база постоянен мониторинг и анализ на ползването му. Съответно, комуникационната свързаност на Единната електронно съобщителна мрежа на държавната администрация ще расте както като покритие, за да достигне до всички публични институции на територията на страната, така и като скорости от 100 гбс и нагоре по основните комуникационни магистрали. Ще се приложат иновативни технологии за интелигентно управление и киберзащита на тази споделена информационна среда и нейното интегриране в националното киберпространство в партньорство с водещите интернет доставчици и телекоми.

Чрез налагането на дисциплина на **централизиран мониторинг и контрол върху разходите** за ИКТ и електронно управление, ще се търси оптимизация на финансовите ресурси за постигане

на максимално ефективно съотношение между стойност и качество на електронното управление.