Политики и архитектури за информационна сигурност на гражданите като потребители на електронното правителство

гл.ас. д-р Антон Палазов
УНСС, катедра „Информатика”
e-mail: apalazov@dir.bg

Резюме: Широкото разпространение и пълноценната функционалност на услугите на електронното правителство, предназначени за българските граждани, ги излагат на рискове от обща загуба на достъпност до тези услуги, включване в атакуващи мрежи, кражба на самоличност, разкриване на тяхна конфиденциална информация и претърпяване на непосредствени финансови загуби.

В статията е показано, че към политиката за информационна сигурност на гражданите могат да се предявят специфични изисквания за минимална задължителна компютърна квалификация, за минимални нива на необходимите разходи за прилагане на политиката и за облекчена еволюция на политиката заедно с прогреса на потребителя при използване на електронните административни услуги. В зависимост от степента на развитие на използваните услуги политиките за информационна сигурност на гражданите са обобщени в три категории: за базови потребители на електронни административни услуги, за идентифицирани потребители и за универсални потребители.

Ясното разграничаване на функционалността на системата за непосредствена защита, средствата за управление и средствата за контрол и налагане на политиката за информационна сигурност позволява в статията да се предложат различни архитектури, които дават определени възможности на гражданите и подпомагат прогреса на електронното правителство. Очертани са главните предимства на архитектурите с централизирани средства за управление и общи средства за непосредствена защита и са специфицирани задължителните функции на софтуерния агент за сигурност като основа за реализация на предлаганите решения.

Ключови думи: електронни административни услуги, политика за информационна сигурност, управление, контрол и непосредствена защита на сигурността, архитектури за защита на информационната сигурност на гражданите, софтуерен агент за сигурност.

JEL: L86, H83.

Търсене на решение на съществуващите проблеми в областта на предоставянето на обществени услуги и в отговор на изискванията за качествено подобряване на тяхната достъпност

при ограничаване на разходите и повишаване на ефективността като фактор, стимулиращ икономическото развитие, правителствата проявяват засилен интерес към концепцията за „електронно" правителство (е-правителство, е-администрация, e-Government). Най-кратко то се определя като масирано използване на информационни технологии, базирани главно върху интернет, при предоставянето на обществени услуги по качествено по-удобен за потребителя, по-ефективен от гледна точка на разходите и принципно различен начин [1]. Тази концепция се стреми да обхване в максимална степен както взаимоотношенията на публичната администрация с гражданите, бизнеса и обществените структури от неправителствения сектор, така и вътрешните взаимодействия и процедури между обособените нейни звена.

Сред основните принципи, върху които се изгражда концепцията за електронно правителство, от особено значение са:

• Принципът за **всеобхватност на предоставяните услуги**, поставящ като цел на електронното правителство достъпността чрез интернет на всички услуги, осъществявани от всички структури в публичната администрация, с тенденция това да стане единственият начин за тяхното получаване.
• Принципът на **всеобхватност на осигурявания достъп**, съгласно който правителствата трябва да осигурят лесен и универсален достъп до електронните административни услуги за всички техни потенциални потребители независимо от тяхното местожителство, пол, доходи, етническа принадлежност, възраст или образование. Лесната достъпност на услугите е и необходимо условие за превръщане на интернет базираните решения в единствена форма за тяхното получаване.

В различни източници възможността за използване на услугите на електронното правителство се свързва единствено с наличието на достъп до компютърна система и комуникационна среда (телефонна линия, високоскоростна връзка чрез кабелна телевизия или локална мрежа, безжична или сателитна връзка). Практическата реализация на тази концепция се осъществява в условия на постоянно увеличаване на заплахите за сигурността на компютърните системи, усъвършенстване на методите и техниките за атаки срещу нея и възникване на многобройни инциденти, причиняващи значителни щети. За противодействие на рисковете за сигурността на информационните системи са разработени множество технологии и софтуерни инструменти, утвърдени са значителен брой стандарти, създадени са подробни политики за сигурност, реализирани са редица мащабни проекти. Преобладаващата част от тях е насочена към гарантиране на безопасността на ресурсите (компютърни системи, данни, приложения, мрежови капацитет), които предоставят услугите на електронното правителство, докато решаването на проблемите с информационната сигурност на потребителите на тези услуги е оставена на заден план. И докато бизнес организациите притежават определен потенциал (бюджет, наличие на квалифициран специализиран персонал, информирани крайни потребители) за самостоятелно справяне със заплахите за сигурността на информационните системи, по-голямата част от гражданите не могат да си позволят подходите, прилагани в големите корпорации.

Целта на настоящата статия е да потърси отговор на следните въпроси, свързани с информационната сигурност на гражданите като потребители на услугите на електронното правителство:

• Съществуват ли рискове за информационната сигурност на гражданите при използване на услугите на електронното правителство и кои са най-важните от тях?
• Необходимо ли е да се разработят специфични политики за сигурност, отнасящи се до гражданите като самостоятелна категория потребители на услугите на електронното правителство, и кои са техните основни елементи?
• Могат ли да се предложат подходящи архитектури на системата за информационна сигурност, които да гарантират, че разработените политики за сигурност са достъпни за гражданите и в действителност се прилагат от тях?

В търсене на отговор на поставените въпроси ще бъдат анализирани текущото състояние и тенденциите в развитието на услугите на електронното правителство, натрупаният опит от страните в ЕС, които са постигнали по-значителен напредък в реализацията на тази концепция, както и съвременните разработки на технологичните лидери и водещите изследователски структури в областта на сигурността на информационните системи.

1. Рискове за информационната сигурност на гражданите при използване на услугите на електронното правителство

Наличието или отсъствието на рискове за информационната сигурност на гражданите зависи в значителна степен от услугите, които електронното правителство реално им предоставя или ще бъде в състояние да предоставя в обозримо бъдеще. Обхватът на тези услуги за българските граждани е очертан в Стратегията за електронно правителство, утвърдена в края на 2002 г. В нея е формулиран набор от 12 индикативни административни услуги, които са от най-съществен интерес за гражданите като масовост на използване, сложност на регламентираните процедури и значимост за общата удовлетвореност от качеството на обслужването. Сред тези услуги, съответстващи на включените в инициативата на ЕС eEUROPE 2002, са [2]:

• подоходни данъци (декларации, уведомяване за резултатите);
• търсене на работа в бюрата по труда;
• социални осигуровки, помощи за безработица, добавки за деца, медицински разходи, стипендии;
• лични документи (лични карти, свидетелства за управление на МПС);
• регистрация на МПС (нови, използвани, внесени МПС);
• подаване на документи за строителни разрешителни;
• заявления към полицията;
• обществени библиотеки (каталози, машини за търсене);
• свидетелства (за раждане, за встъпване в брак и др.);
• дипломи за средно и висше образование;
• адресна регистрация;
• услуги, свързани със здравеопазването (съвети за наличността на определен тип услуги в различни болници, запазване на час за преглед).

Доколкото всяка от изброените услуги може да се реализира към определен момент с различна степен на обхват и функционалност, за оценка на постигнатото равнище по отношение на конкретна услуга, както и за измерване на прогреса на всяка от държавите – членки на ЕС, в областта на електронното правителство се прилага скала от 4 степени (нива):

- първа степен: потребителите получават само информация за съответната услуга – правна рамка, регламентирани процедури, необходими документи;
- втора степен: потребителите могат да осъществяват еднопосочна комуникация, като зареждат от съответните сайтове електронни копия на необходимите им формуляри или получават справки за тяхното персонално състояние (внесени социални осигуровки, здравноосигурителен статус, изплатени обезщетения за временна нетрудоспособност и др.);
- трета степен: „електронното правителство" позволява двупосочно взаимодействие с гражданите, при което те могат както да изпращат електронни изявления (заявки за обслужване) с правна стойност към съответните административни органи, така и да получават от тях обратна информация;
- четвърта степен: в допълнение към двупосочната комуникация от предишната степен гражданите и административните органи са в състояние да осъществяват електронни разплащания (когато са необходими за съответната услуга), както и да получават електронни доставки на документи с правна стойност.

Към настоящия момент електронното правителство в България предоставя на гражданите информация за част от услугите в индикативния списък, възможност за „сваляне" на формуляри, необходими за някои от тях, получаване на персонални справки за внесените осигуровки и здравноосигурителен статус. Като най-добре развити могат да се определят услугите, които позволяват подаване на декларации за облагане на гражданите с подоходни данъци, както и промяна в адресната им регистрация. От текущото състояние на услугите на електронното правителство в България може да се направи извод, че в преобладаващата си част те са достигнали до втора степен от четиристепенната скала; относително малка част позволяват по-сложни взаимодействия с административните органи, а за някои от тях (например тези, свързани със здравеопазването) още липсва ясна концепция.

Същевременно опитът на други държави от ЕС [5], [6] показва, че услугите за гражданите вече са достигнали до трета и четвърта степен и се полагат целенасочени усилия за тяхното популяризиране и утвърждаване на това равнище. Инициативата на Европейската комисия i2010 Европейско информационно общество за растеж и заетост [3] поставя акцентите в областта на електронното правителство върху предоставянето на по-пълноценни и завършени административни услуги, които са достигнали в своето развитие до трета или четвърта степен от дефинираните по-горе.

Подобни амбициозни изисквания поставя и приетият през 2007 г. в България Закон за електронното управление [4]. Той задължава административните органи да предоставят всички услуги в рамките на тяхната компетентност и по електронен път. Те не могат да отказват приемането на електронни документи, които са издадени и подписани съгласно изискванията на Закона за електронния документ и електронния подпис, както и да отказват издаването на електронни документи и извършването на електронни административни услуги. Законът предвижда и регламентиране на начините за електронни разплащания по повод на тези услуги. Като получатели на електронни административни услуги гражданите имат право да изпращат (например чрез публично достъпно WEB базирано приложение) електронни документи, подписани с електронен подпис, който се използва за установяване на авторството и целостността на електронните изявления.

Изложеното по-горе дава основание да се смята, че и електроното правителство в България ще се развива в посока на повишаване на качеството на предоставяните електронни административни услуги, което предполага реализация на по-сложни модели на взаимодействие между гражданите и административните органи, свързани с обмен на електронни документи, електронни разплащания и доставки.

Като потребители на услугите на електронното правителство гражданите взаимодействат с него по два основни начина:

- Чрез работни места в телецентрове, изградени в офисите на местната и държавната администрация, в клоновете на банки или на други места. При тази форма на достъп до услугите дейностите по защита на сигурността на информацията ще се осъществяват от специализирани в тази област екипи, които ще получават и необходимата финансова и друга подкрепа от страна на държавата. Поради тези особености системите за защита на информационната сигурност на потребителите, използващи възможностите на изградените телецентрове, не са обект на настоящото изследване.
- Чрез домашни компютри, разполагащи с връзка към интернет, или чрез преносими компютри или мобилни устройства, които регламентирано се включват към изградени безжични мрежи. Доколкото в този случай работните станции на потребителите са извън обхвата на ясна и налагана политика по сигурността на някоя организация, степента на защита на тяхната информационна безопасност в значителна степен е в собствените им ръце. В същото време тази форма на използване на електронните административни услуги е най-естествена и се стимулира от инициативите на ЕС. Поради това по-нататъшното изложение се концентрира именно върху такава форма на взаимодействие с електронното правителство.

От очертаното състояние и близки перспективи пред реализацията на услугите на електронното правителство в България могат да се формулират следните по-съществени и вероятни рискове за информационната сигурност на гражданите като техни потребители:

- **Обща загуба на достъпност на услугите на електронното правителство**: в резултат например от действието на вредителски софтуер компютърната система на потребителя губи изцяло работоспособност или се лишава от решаващи нейни елементи (например от възможност за свързване към интернет). Вследствие на това осигурените материални фактори (компютърна система и комуникационна среда) няма да гарантират достъпността на обществените услуги, предоставяни чрез електронното правителство, а гражданинът ще изгуби възможността да ги използва.
- **Включване в атакуващи мрежи**: рисковете за информационната сигурност на гражданите като потребители на услугите на електронното правителство не се изчерпват с възможната загуба на работоспособност от техните работни станции. Нейното компрометиране чрез средства за проникване например създава условия за неявното включване на съответната компютърна система в мрежа за осъществяване на целенасочени атаки, водещи до отказ от обслужване. От тях могат да пострадат например сървърите, реализиращи самите услуги на електронното правителство, което ще отнеме възможността да се използват предоставяните електронни услуги на всички потребители (дори на тези, които притежават адекватна система за

защита на сигурността). Стремителното увеличаване на броя на потребителите на интернет, които не притежават достатъчна степен на защита на сигурността, ще предизвика значителни затруднения и ще окаже негативно влияние и върху цялостното развитие на електронния бизнес. С усъвършенстване на законодателството в тази област гражданите могат да бъдат застрашени и от юридически претенции от страна на пострадали трети страни.

• **Кражба на самоличност**: разкриването на универсалния идентификатор на потребителя (ЕГН) (чрез който той се удостоверява при използване на услугите на електронното правителство) от потенциални нарушители с помощта на техниките на социалния инженеринг, чрез шпионски софтуер или по друг начин им дава възможност да се представят от негово име в транзакциите с административните органи. Така те могат да получат документи за самоличност, да регистрират на чуждо име МПС, да получат юридически валидни копия от актове за раждане и от други документи, изграждащи правната идентичност на гражданина. Притежавайки подобен набор от документи, нарушителите имат възможността да осъществяват всякакви други действия от името на съответното лице, с което да му причинят преки и косвени щети.

• **Разкриване на конфиденциална информация за гражданина**: когато нарушители придобият информация, която се обменя между потребителя и органите, предоставящи електронни административни услуги, чрез социален инженеринг, достъп до вътрешна информация, манипулиране на мрежовия трафик или чрез други техники, те получават възможността да компрометират достоверността на предоставяните от гражданина данни, да използват информацията против жизнените му интереси или като инструмент за кражба на неговата самоличност. В тази ситуация нарушителите могат да нанесат на потребителите не само преки финансови щети, но и да подкопаят тяхното доверие в концепцията за електронно административно обслужване и бизнес.

• **Претърпяване на непосредствени финансови загуби**: когато електронните административни услуги придобият пълната си функционалност и някои от тях включват средства за електронни доставки и разплащания, потенциалните нарушители получават възможност с помощта на шпионски софтуер, пренасочване към фалшиви сайтове, посегателства върху физическата сигурност или чрез други методи да осъществят директно манипулиране с парични средства, които принадлежат на гражданите. По този начин могат да бъдат присвоени възстановявани от администрацията данъци, изплащани помощи при безработица, суми за семейни надбавки и други парични средства, които се предоставят на хора с най-ниска степен на информираност за рисковете пред сигурността.

2. Политики за информационна сигурност на потребителите на електронното правителство

Под политика за информационна сигурност (ПИС) ще разбираме съвкупност от правила, която определя:

• ресурсите, подлежащи на защита, техните потребители и рисковете, приети за съществени по отношение на тяхната сигурност;

• правилата, свързани със сигурността, които потребителите трябва да спазват, и отговорностите, които те носят при тяхното нарушаване;

• елементите на системата за защита на информационната сигурност и изискванията

към тяхното инсталиране, конфигуриране и обновяване;
- средствата за управление на системата за защита и за контрол върху действителното прилагане на политиката за информационна сигурност;
- процедурите за възстановяване на системата за защита при възникване на инциденти със сигурността.

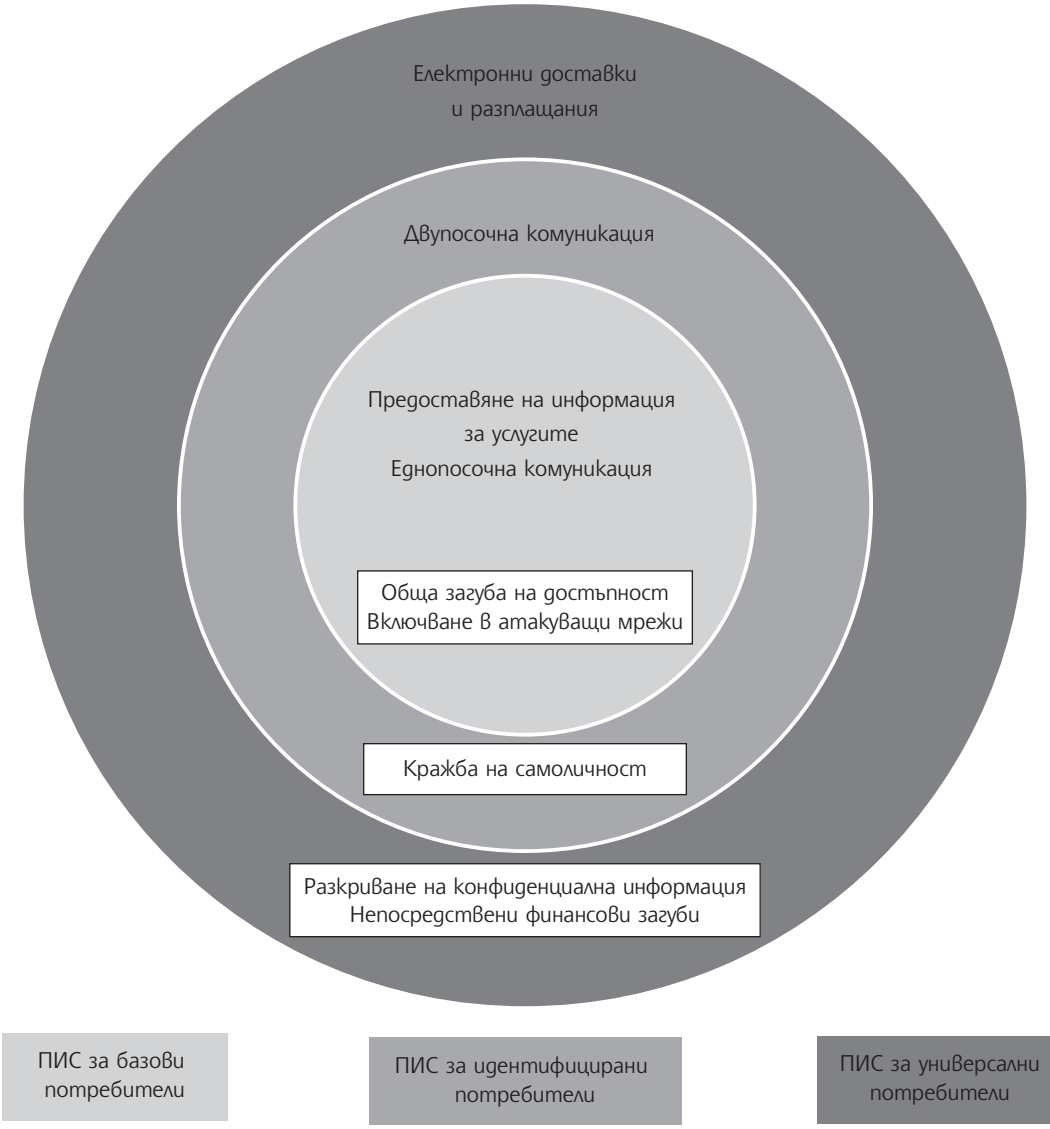
Към политиката за информационна сигурност на гражданите като потребители на услугите на електронното правителство съществуват няколко специфични **изисквания**:

- Минимални задължителни изисквания към квалификацията на потребителите по отношение на инсталирането, конфигурирането, обновяването и възстановяването на елементите от системата за защита на сигурността, които позволяват максимална прозрачност при тяхното използване.
- Минимални изисквания по отношение на необходимите ресурси, които гражданите трябва да осигурят, за да приложат разработената политика и дефинираните в нея средства за защита. Удовлетворяването на това изискване предполага максимална типизация на разработваните решения.
- Възможност за развитие на ПИС заедно с прогреса на потребителя в посока на обогатяване на използваните от него услуги.

За да се дефинират основните категории политики за информационна сигурност на потребителите на електронното правителство, трябва да се анализира връзката между степента на развитие на неговите услуги и вероятността за проявление на определените по-горе основни рискове (фиг. 1). Когато електронните административни услуги се намират на първа или втора степен и тяхното използване се свежда до пасивно потребление на достъпна в интернет информация, основните рискове за гражданите са загубата на достъпност на услугите и включването им в атакуващи мрежи. Работните станции на потребители, за които са достатъчни или са предоставени услуги с такива степени на развитие, се нуждаят от система за защита с базова функционалност, аналогична на тази, предоставяна на крайните точки в големите корпоративни мрежи. Прилаганата за тях политика за информационна сигурност може да се определи като **ПИС на базови потребители**.

Когато гражданите получат достъп до електронни услуги от трета степен и станат част от по-сложни двупосочни комуникации, към посочените по-горе рискове се прибавя опасността от кражба на самоличност. За да отговори на тези предизвикателства, политиката за информационна сигурност на гражданите трябва да се допълни с механизми и технологии за удостоверяване на тяхната идентичност и използване на електронни подписи. Такава политика за информационна сигурност може да се определи като **ПИС на идентифицирани потребители**.

Когато за потребителите на електронното правителство възникне необходимост и им се предостави възможност за използване на пълноценни услуги, които предполагат осъществяване на електронни доставки на документи с юридическа стойност и извършване на електронни разплащания, рисковете от разкриване на поверителна информация за гражданите и претърпяване на непосредствени финансови загуби значително се увеличават. Тогава политиката за информационна сигурност трябва да се разшири с механизми за многофакторна автентикация и криптиране на обменяните данни и може да се определи като **ПИС на универсални потребители**.



Фигура 1. Развитие на електронните административни услуги и рискове за информационната сигурност

Определените чрез политиката софтуерни средства за запазване на информационната сигурност могат да се класифицират според тяхното предназначение в 3 основни групи:

• **Средства за реализация на политиката за информационна сигурност** – представляват софтуерни инструменти и технологични решения, които предпазват от осъществяване на атаки срещу сигурността, откриват възникването на инциденти и реагират срещу тях с цел отстраняване на проникването, предотвратяване на по-нататъшното разпространение и

възстановяване на нормалното състояние на системата. Често тази съвкупност от инструменти и технологии се нарича **система за защита** на сигурността.

• **Средства за контрол и налагане на политиката за информационна сигурност** – чрез тях се установява доколко текущото състояние на системата за защита е адекватно на утвърдената политика за информационна сигурност и при необходимост се предприемат действия за привеждането им в съответствие.

• **Средства за управление на системата за защита на сигурността** – чрез тях се определят структурните елементи на системата за защита и се конфигурират техните съществени параметри. По такъв начин се създава формализирано описание на цялостната политика за информационна сигурност, което позволява по софтуерен път да се упражнява контрол за съответствие и да се налага нейното фактическо прилагане. Често тази група от средства се нарича единна **конзола** на системата за защита на сигурността.

Както вече бе посочено по-горе, системата за защита на базови потребители е близка по своите възможности на тази, реализирана за крайните точки (стационарни и преносими компютри) в корпоративните мрежи (endpoint protection). Според изследванията на Symantec [7] тя трябва да съдържа следните елементи:

• **антивирусен софтуер**, който открива чрез разпознаване на сигнатури, в реално време или при сканиране компютърни вируси, червеи, троянски коне, шпионски софтуер и други форми на вредителски код върху устройствата на крайната точка и отстранява заразяването, като изтрива, поставя под карантина или възстановява в първоначално състояние поразените обекти;

• **защитна стена**, която контролира мрежовия трафик и предпазва както от отдалечено проникване в работната станция, така и от по-нататъшно разпространение на вредителския код в мрежата;

• **технологии за превантивна защита** (proactive protection technologies), които са предназначени да противодействат на нововъзникнали или модифицирани заплахи чрез евристични методи за анализ на поведението на приложенията, устройствата и потребителите и търсене на съмнителни техни действия.

С**редствата за управление** на системата за защита са предназначени да дефинират набор от компоненти, реализиращи безопасността, както и допустимите стойности на техни съществени параметри. В зависимост от обхвата на защитаваната информационна система средствата за управление могат да събират и анализират данни за протичащите в нея събития, свързани със сигурността, както и да оптимизират процесите по обновяване на други компоненти.

Сред по-важните характеристики на политиката за информационна сигурност, които подлежат на описание, контрол и налагане, са:

• задължително активни компоненти от системата за защита на сигурността и допустими стойности на някои техни ключови параметри;
• изисквания към честотата на обновяване на инструментите за защита, към обхвата на обновяването, към разрешените източници на актуализации;
• режим за контрол върху критични от гледна точка на сигурността устройства;
• ограничения върху достъпността на приложения или отделни техни функции, на информационни ресурси, сайтове и т.н.

Средствата за контрол и налагане на политиката за информационна сигурност трябва да осъществяват следните основни функции:

- Събиране в реално време на **информация за текущото състояние** на компонентите от системата за защита на сигурността, както и за конфигурирането на ключови техни параметри – активни и неактивни компоненти, степен на актуалност, включени и изключени възможности, достъпни и недостъпни ресурси, разрешени и забранени към момента действия.
- **Проверка за степента на съответствие** между текущото състояние на системата за защита и предписанията в политиката за информационна сигурност. В зависимост от резултатите от проверката средствата за контрол установяват, че сигурността е с адекватен статус или че регистрираните отклонения налагат предприемане на допълнителни действия.
- **Налагане на политиката** за информационна сигурност при наличие на съществени различия между нея и състоянието на контролираната система за защита. Налагането на политиката може да включва активиране на компоненти за защита, промяна в настройката на техни параметри, извършване на обновяване на компонентите (зареждане на по-нови версии, промяна на сигнатури и дефиниции, влияещи върху тяхната работа), забрана за използване на устройства, приложения или други ресурси.
- **Маршрутизиране** към единната колона на постъпващата от компонентите на системата за защита информация за събития, свързани със сигурността.

3. Архитектура на системите за информационна сигурност на потребителите на електронното правителство

След пълноценна реализация на услугите на електронното правителство броят на неговите потребители трябва да достигне до стотици хиляди или дори до милиони. Прилагането на класическите решения в областта на информационната сигурност за всеки от тях означава, че огромен брой граждани трябва да познават изискванията по отношение на безопасността за различните електронни административни услуги, поотделно да лицензират, инсталират, конфигурират и обновяват необходимите инструменти за защита на сигурността и да осъществяват задължителните изменения в тях в процеса на развитие или разширяване на услугите. Подобен подход не съответства на формулираните по-горе специфични изисквания към политиките за информационна сигурност на гражданите, свързани с минимизиране на очакванията за тяхната квалификация, ограничаване на задължителните разходи и лесната им еволюция в процеса на използване на електронни административни услуги.

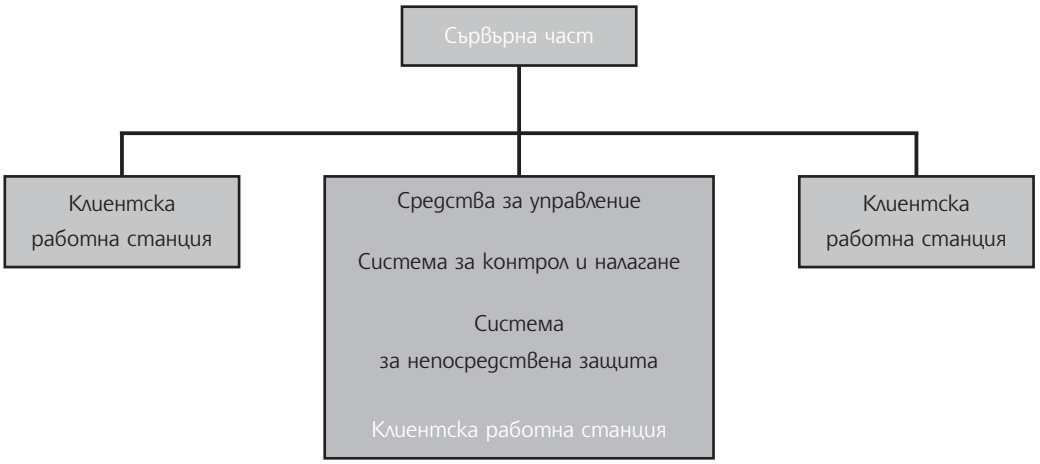
Намирането на решения, които са адекватни на тези специфични изисквания, предполага централизиране на някои от елементите на системата за информационна сигурност. Това означава, че тя ще се постига чрез някакво съчетание между общи за всички потребители компоненти, функциониращи като сървърна част на системата, и специфични за всеки от тях елементи, наричани по-долу клиентска част. Централизирането на компоненти може да се осъществи в следните насоки:

• **Централизиране на експертизата**: сървърната част предоставя формализирани описания на изискванията към информационната сигурност при използване на различни електронни административни услуги, които се създават от професионалисти в тази област и се използват от всички потребители на съответните услуги заедно със софтуерни средства за автоматичен контрол и налагане в клиентската част.

• **Централизиране на общи инструменти** за защита на информационната сигурност: сървърната част предоставя възможност за автоматично инсталиране и конфигуриране върху клиентските работни станции на средства за защита на сигурността преди получаване на достъп до определени услуги на електронното правителство. По този начин се постига съществено ограничаване на задължителните разходи за лицензиране на софтуерни инструменти за защита на информационната сигурност, гарантира се оптимална настройка при тяхното използване и се предоставя надежден източник за обновяване.

Централизирането на експертиза и на инструменти за защита представлява форма на предоставяне на непосредствени услуги, свързани с информационната сигурност на гражданите като потребители на електронното правителство, и предполага осигуряване на необходимите за това човешки и финансови ресурси.

В зависимост от степента на централизация на средствата за управление, за контрол и налагане и за непосредствена защита, както и при отчитане на съвременните технологични възможности, могат да се дефинират различни **архитектури** на системата за информационна сигурност на гражданите. Те се отличават по това, дали съответната функционалност се включва като елемент от клиентската или от сървърната част на решението, по разпределението на натоварването между сървърите, клиентските работни станции и комуникационната инфраструктура, по средните нива на разходите за защита на клиентска работна станция, както и по изискванията към квалификацията на крайните потребители при управление, контрол и използване на средствата за защита.



Фигура 2. Монолитна архитектура на системата за информационна сигурност

При съобразяване с формулираните по-горе изисквания и ограничения системата за информационна сигурност на гражданите може да се изгради чрез някоя от следните архитектури:

• **Монолитна –** за нея е характерно, че липсва централизация и всички функции по защита, контрол и управление на информационната сигурност се реализират самостоятелно на всеки отделен възел (клиентска работна станция) [9]. Инструментите и технологиите за защита са инсталирани във всяка крайна точка, тяхната настройка и конфигуриране се осъществяват чрез потребителската конзола, всички необходими актуализации трябва да се пренесат и извършат върху всеки от възлите (фиг. 2). Възможностите за едновременна промяна в политиката за сигурност на множество крайни точки са силно ограничени.

На монолитната архитектура са присъщи редица недостатъци:

- изискванията към компютърната квалификация на потребителите значително надвишават нейното средно равнище за България;
- необходимостта от инсталиране на целия набор от софтуерни инструменти на всяка работна станция значително увеличава средните разходи за тяхното притежаване на една крайна точка;
- затрудненото едновременно изменение в параметрите на сигурността за множество работни станции води до значителни проблеми при еволюцията към по-развита политика, отговаряща на използваните от гражданите по-усъвършенствани електронни административни услуги.

• **Архитектура с централизирано управление** – за разлика от монолитната архитектура, при тази с централизирано управление функциите по управление на средствата за защита на сигурността на клиентските компютри е изнесена в сървърната част (фиг. 3). Средствата за контрол и непосредствена защита продължават да бъдат разположени върху крайните точки.

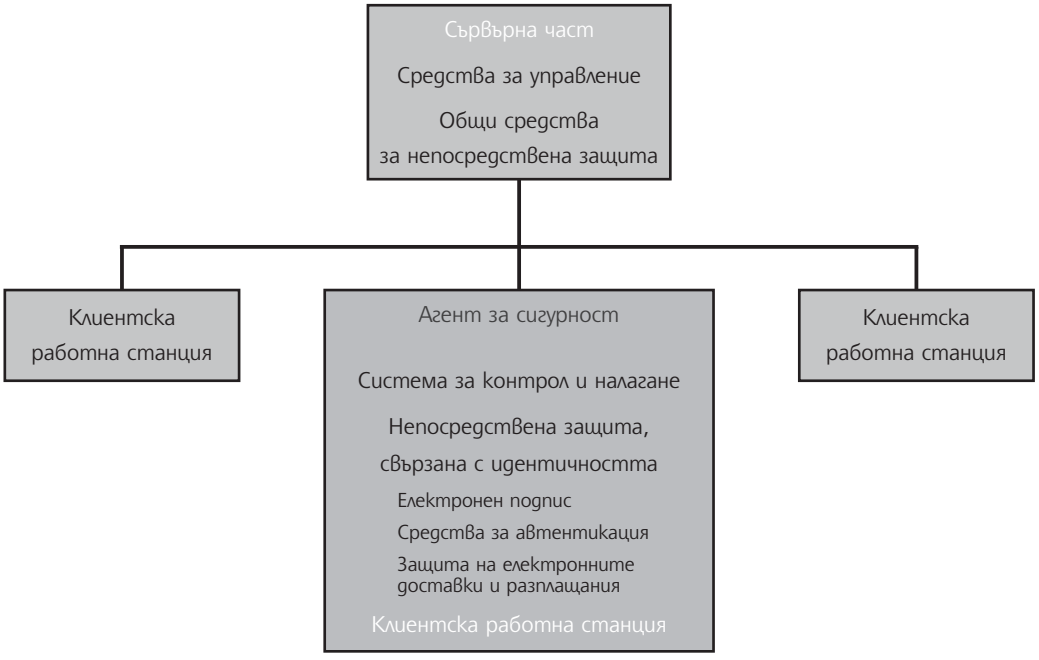
Фигура 3. Архитектура с централизирано управление на системата за информационна сигурност

Специализиран конфигурационен агент, инсталиран на потребителските компютри [8], взаимодейства с централизираното управление, като получава формализирани описания на политики за информационна сигурност, актуализации на различни софтуерни инструменти, сигнали за непосредствени заплахи и др.

Архитектурата с централизирано управление предоставя на потребителите на електронни административни услуги възможност за използване на най-добрите конфигурации на съответните инструменти за защита и облекчава тяхното преминаване към други политики за информационна сигурност. Наред с това тя продължава да съдържа съществени недостатъци:

- изискванията към компютърната квалификация на потребителите остават достатъчно високи;
- запазва се необходимостта от лицензиране и инсталиране на значителен набор от софтуерни инструменти на всяка работна станция, което задържа средните разходи за тяхното притежаване в една крайна точка на достатъчно високо ниво.

• **Архитектури с централизирани управление и общи средства за защита –** в сравнение с предишната разгледана архитектура се предлага като сървърни услуги да се реализират и част от общите средства за непосредствена защита на сигурността (фиг. 4). В крайната точка се запазват само тези от инструментите, които са пряко свързани с идентичността на потребителя (средства за автентикация и електронен подпис, криптографски технологии и технологии за защита на електронните доставки и разплащания).



Фигура 4. Архитектура с централизирани управление и общи средства за защита на системата за информационна сигурност

Софтуерен агент, представляващ функционална част от системата за контрол и налагане на политиката за информационна сигурност и активиран автоматично от операционната система, получава от компонентите за централизирано управление нейното формализирано описание и проверява текущото състояние на защитаваната клиентска работна станция. Ако състоянието е удовлетворително, агентът осъществява зареждане и стартиране на предвидените инструменти за защита в реално време. Когато резултатите от проверката са незадоволителни, същият агент активира централизирано съхранявани инструменти за диагностициране и отстраняване на несъответствията.

Архитектурите с централизирани управление и общи средства за защита предоставят значителни предимства на потребителите на услугите на електронното правителство:

- изискванията към тяхната компютърна квалификация са минимални, особено докато те остават базови потребители на услуги според класификацията, предложена по-горе (най-многобройната сега и в близка перспектива група от потребители);
- политиката за информационна сигурност на базовите потребители ще изисква инсталиране на минимален набор от софтуерни инструменти на всяка работна станция, който в идеалния вариант може да съдържа само споменатия по-горе софтуерен агент; по този начин средните разходи за прилагане на политиката в една крайна точка съществено ще се намалят, което ще я направи достъпна за всички граждани;
- възможностите за миграция от една към друга политика за информационна сигурност са ограничени единствено от функционалността на използвания софтуерен агент и могат да се осъществяват прозрачно за потребителите от професионалисти, разполагащи с експертиза в тази област.

В заключение могат да се направят следните **изводи**:

- пред гражданите като потребители на електронни административни услуги съществуват значими за тяхната информационна сигурност рискове, които се увеличават с прогреса на електронното правителство;
- тенденциите в развитието на услугите на електронното правителство позволяват да се дефинират категории от политики за информационна сигурност, отнасящи се до базови, идентифицирани и универсални потребители, които притежават както различия в задължителната функционалност, така и общи изисквания към тяхната приложимост;
- най-подходящи за защита на информационната сигурност на гражданите от гледна точка на приложимостта са архитектурите с централизирани управление и общи средства за непосредствена защита, като тяхната ефикасност се влияе в значителна степен от функционалността на агента за сигурност, работещ върху клиентската работна станция;
- реализацията на разгледаните политики и архитектури за информационна сигурност на гражданите като потребители на електронното правителство изисква и предоставяне на непосредствени **услуги** от държавата и общините, които да увеличат в максимална степен достъпността на технологиите – както достъпността на интернет за всички граждани и компании е основен фактор за успеха на електронното правителство, така и универсалната достъпност на услугите, свързани със сигурността, е с решаващо значение за неговата жизненост.

Литература

1. Холмс, Д., Стратегии за електронно правителство., С., Класика и стил, 2002.

2. Стратегия за електронно правителство, 2003.

3. European Commission (2006). i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions.

4. Закон за електронното управление, ДВ, бр. 26/2007 г.

5. ePRODAT: e-Government and Data Protection in European Regions and Cities, 2006.

6. Rupp, Ch., E-Government in Austria., 2005.

7. Symantec Corporation. Symantec Endpoint Protection. A unified, proactive approach to endpoint security, 2007.

8. Intel Information Technology. Integrated Software Enhances Enterprise Security, 2006.

9. Microsoft Corporation. Microsoft TechNet: Antivirus Defense-in-Depth, 2004. ИА