



РЕПУБЛИКА БЪЛГАРИЯ  
МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

---

## ИНСТРУКЦИЯ

### За попълване на приложение №1 към чл. 38, ал.3 от НОИИСРЕАУ

#### Контекст

Настоящата инструкция е изготвена от екипа на Дирекция МИС на Министерство на електронно управление с цел да разясни и подпомогне дейността по попълване на приложение №1 към чл. 38, ал.3 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ) при изготвянето на технически спецификации в контекста на изисквания за мрежова и информационна сигурност.

Един от основните казуси при изготвяне на техническа спецификация е по какъв начин и къде да бъдат описани изискванията за мрежова и информационна сигурност. След въвеждането на необходимостта от включване на изискванията по Наредбата за минимални изисквания за мрежова и информационна сигурност (НМИМИС) в техническите спецификации, при изготвянето им беше възприет подход за изписване на изискванията на едно място. Практиката е те да бъдат включени ли в *т. 7.2.7 Информационна сигурност и интегритет на данните* или в *т. 7.2.10 Изисквания за киберсигурност*. Въпреки, че не е задължително, практиката показва, че едно подобно изписване на изискванията значително улеснява както изготвящите, така и проверяващите.

Друг казус при изготвяне на технически спецификации е как да бъде отразено в текста когато едно изискване е вече изпълнено от съществуващата архитектура. От страна на проверяващия, за да може да бъде достигнато до заключението, че изискването е вече изпълнено, в техническата спецификация трябва ясно, конкретно и в пълен обем да е описано по какъв начин то е реализирано.

Важно е да се отбележи, че в случаите, когато определено изискване вече е задоволено, по един или друг начин, от съществуваща инфраструктура, **не означава** че е НЕПРИЛОЖИМО за ТС, тъй като в случаите, когато, поради една или друга причина, тази инфраструктура се промени, **не се гарантира** изпълнението на изискваната по закон функционалност посредством ТС в новата инфраструктура.

В следващите точки се разглеждат различните изисквания, включени съгласно НМИМИС.

- 1. Включени ли са адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване. (Чл. 12, ал.1 от НМИМИС)?**

Анализът и оценката на риска са основополагащите елементи, посредством които се идентифицират рискове и конкретни заплахи за информационната система (не за изпълнението на самия проект!). Въз основа на така идентифицираните рискове и заплахи, следва да се въведат механизми за тяхното смекчаване с цел постигане на определено ниво на сигурност на информацията, мрежата или информационната система. Основно водещо

---

правило при имплементиране на смекчаващи механизми е използването на такива, които са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

Като проверяващи, ние очакваме в техническата спецификация да бъдат включени изисквания за конкретни адекватни и пропорционални на рисковете смекчаващи механизми, които се основават на анализ и оценка на риска. Естествено, за да можем да стигнем до заключението, че смекчаващите механизми се основават на анализ и оценка на риска, подобни трябва да бъдат включени в техническата спецификация. Това трябва да бъде описано по ясен и еднозначен начин, като има ясно аргументирана връзка между механизмите и анализа и оценката на риска.

Обръщаме внимание, че тук става въпрос за оценка и анализ на риска за изгражданата система, а не за такъв на проекта като цяло.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира еднозначен запис със специфични изисквания за смекчаване на рисковете, основан на анализ и оценка на риска. Също е приемливо, ако този запис фигурира като изискване за изпълнение от страна на Изпълнителя по договор.

Не се предвиждат случаи, в които тази точка да бъде НЕПРИЛОЖИМА за определена техническа спецификация. Ако в процеса на работа подобен случай възникне, причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

## **2. Представени ли са анализ и оценка на риска, които да служат като основа за включването на адекватни и комплексни изисквания за мрежова и информационна сигурност по т.1.**

Докато първото изискване говори за представяне на механизмите, произлезли от анализа и оценката на риска, настоящото изискване се отнася пряко за тези реквизити. Тяхното включване трябва да залегне в техническата спецификация, за да може контролиращият да се увери, че механизмите в изложените текстове съгласно изискването по чл. 14, ал.1 от НМИМИС са адекватни, пропорционални на рискове и са залегнали още на етап техническа спецификация.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурират анализ и оценка на риска за разработваната информационна система. Също е приемливо, ако този запис фигурира като изискване за изпълнение от страна на Изпълнителя по договор.

Не се предвиждат случаи, в които тази точка да бъде НЕПРИЛОЖИМА за определена техническа спецификация. Ако в процеса на работа подобен случай възникне, причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

### *Филтриране на трафика*

## **3. Предвидено ли е ненужните портове по протоколи Transmission Control Protocol (TCP) и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика?(Чл.14, ал.2 от НМИМИС)**

Защитата на портовете е фундаментален защитен механизъм, посредством който да бъдат защитени информационните системи от различни видове зловредни атаки. Имплементацията на подобен механизъм може да бъде реализирана по разнородни начини, включително да бъде гарантирана от вече съществуваща архитектура.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване за забрана на ненужните портове. Също е приемливо, ако този запис фигурира като изискване за изпълнение от страна на Изпълнителя по договор. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които става въпрос за вътрешна система, която не се достъпва през Интернет. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

#### *Среда за администриране*

- 4. Предвидено ли е използването на отделна, изолирана от другите информационни и комуникационни системи и от интернет, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти? Тази среда трябва да не се използва за други цели.**

Средата за администриране на системата е един от ключовите елементи за гарантиране на нейната сигурност и за проследимост в случай на инцидент. Ако например връзката до административния панел се осъществява без криптиране или под друга незащитена форма, вероятността сигурността на системата да бъде компрометирана, заедно с информацията в нея, се увеличава експоненциално. Друг случай е когато средата се използва и за други цели, освен администриране на системата, което може да доведе до нейното компрометиране по тази друга линия.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване за използване на отделна, изолирана от другите информационни и комуникационни системи и от Интернет, подходящо защитена среда за целите на администриране, като тя не трябва да се използва за други цели. Също е приемливо, ако този запис фигурира като изискване за изпълнение от страна на Изпълнителя по договор. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които става въпрос изцяло автоматизирана система, която не изисква администриране. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

#### *Защита на уеб сървъри*

- 5. Предвидена ли е валидация на всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на брауъра, като headers на препращащия и потребителски агент?(чл. 24, т. 6)**

Валидирането на данни на входа, известно още като валидиране на данни, е тестване на всеки вход за коректното интерпретиране на всички входните данни. Валидирането на входа предотвратява навлизането на неправилно формирани данни в информационната система. Валидирането на входа трябва да се извършва, когато данните се получават от външна страна, като неправилното валидиране на входа може да доведе до атаки с инжектиране на код, изтичане на памет и компрометиране на системи. Всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на брауъра трябва да бъдат валидирани и да бъде забранено въвеждане на специални символи от страна на потребителя.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване за това всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на брауъра да бъдат валидирани и да бъде забранено въвеждане на специални символи от страна на потребителя. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които няма функционалност за въвеждане на данни от страна на потребителя.

---

Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**6. Предвидено ли е всички данни да бъдат кодирани с HTML, изпращани от клиента и показвани в уеб страница? (Чл. 24, т. 8)**

За да може информацията да бъде представяна коректно както пред потребителя, така и пред сървър, всички данни трябва да бъдат кодирани в HTML посредством един от т.н. набори от символи (character set), използвани за кодиране в HTML. Некоректното кодиране може да доведе до редица проблеми включително до cross site scripting атаки.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване предвиждащо всички данни да бъдат кодирани с HTML. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които описваната информационна система не е свързана с Интернет. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**7. За защита от атаки от типа отказ от услуги (DOS):**

**а. Предвидено ли е ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL?**

Ограничаването на максималната дължина на заявката се налага с цел предотвратяване на атаки от потребители, които публикуват големи файлове на сървър. По подразбиране големината на заявката е лимитирана до 2 MB, но при специфична необходимост може да бъде коригирана с подходяща за целта стойност.

С ограничаване на дължината на целият URL, включително заявката, до максимум 2048 символа се добавя допълнителен слой защита с цел да се предотврати уязвимостта от DDOS атака на slow HTTP Request на уеб сървър. Дължината само на заявката по URL следва да е не повече от 1024 символа.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване предвиждащо ограничаване на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които описваната информационна система не е свързана с Интернет. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**б. Предвидено ли е конфигуриране на типа и размера на headers, които уеб сървърът ще приеме?**

За предотвратяване на DDoS атаки към уеб сървър, системата трябва да бъде еднозначно параметризирана със стойности на типа и размера на headers, които ще бъдат приемани като заявки от клиента.

Например, параметърът max-http-header-size (по подразбиране е конфигуриран за Apache на 8K, nginx на 8K, IIS на 8-16K, на Tomcat на 8-64K) да бъде конфигуриран в разумни граници, така че при DDoS атака с множество заявки с прекалено голям размер на header payload да не доведе до изчерпване на наличните ресурси на сървър, което да доведе до невъзможност и отказ от изпълнение на основните му функции.

Също така, деактивирането на неизползваните headers, и параметризирането останалите в препоръчителни граници (напр. max-age = seconds, keep-alive, type/content и т.н.), за да бъдат предотвратени бъдещи DDoS атаки.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване за това типът и размерът на headers, които уеб сървърът ще приеме, да бъдат конфигурирани в разумни граници. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които описваната информационна система не е свързана с Интернет. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**в. Предвидено ли е да се ограничи времетраенето на връзката (connection Timeout), на времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и на минималния брой байтове в секунда при изпращане на отговор на заявка?**

Ограничаването на изчакването на заявките от страна на сървъра (т.н. connection timeout) е механизъм за защита от атаки от вида DDOS, при които се насочват огромен брой заявки, целящи да започнат отваряне на връзка със сървъра, заемане на ресурс от негова страна (изчислителна мощ, оперативна памет), но никога да не бъдат затворени, водейки до изчерпване на наличните ресурси на сървъра и съответна негова невъзможност да изпълнява първоначалната си функция.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване за това да се ограничи времетраенето на връзката, на времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и на минималния брой байтове в секунда при изпращане на отговор на заявка. Ако това изискване е вече изпълнено от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които описваната информационна система не се предвижда да работи в Интернет. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**8. Предвидено ли е да се въведе ограничение на броя неуспешни опити за влизане в системата?**

За защита от атаки от вида brute force, чрез които се цели да се придобие достъп до определен потребител (като например администратор), в техническата спецификация трябва да се предвиди функционалност за разумна защита от многократни опити за влизане в системата с профил на един потребител за определен период от време.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които системата няма предвидени потребители (*забележка: сам по себе си, администраторът е потребител с администраторски права*). Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**9. Предвидено ли е да не се допуска извеждането на списък на уеб директориите;**

Извеждането на списък с уеб директориите е функция на уеб сървърите, която показва съдържанието им, когато няма индексен файл (index file) в конкретна директория. Подобна

---

функция е опасно да бъде оставена тъй като води до разкриване на информация, включително информация за всичко, което се намира на уеб сървър.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване да не се допуска извеждането на списък на уеб директориите. Ако тези изисквания са вече изпълнени от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които системата не включва изграждането(или надграждането) на уеб сайт. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

#### **10. Предвидено ли е бисквитките (cookies) задължително да имат:**

- а. флаг за защита (security flag), който инструктира брауъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали;**
- б. флаг HTTP only, който инструктира брауъра, че „бисквитката“ може да бъде достъпна само от сървъра, а не от скриптовете от страна на клиента;**

Основната цел на бисквитките е да бъде установена персистентност на връзката между потребителя и сървър. Това предоставя удобство както на потребителя, така и възможност за извършване на по-задълбочени анализи на поведението му. В този смисъл, бисквитката представлява важна част от комуникацията между потребителя и сървър, затова към нея са заложили специфични изискванията в НМИМИС, конкретно включването на два флага Set-cookie – HttpOnly и Secure. HttpOnly флагът е допълнителен флаг, в Set-Cookie, използването на който при генерирането на бисквитка спомага да се намали риска от това тя да бъде достъпна от клиентски код, например, бисквитката не може да бъде достъпена от Javascript. Като резултат, дори ако съществува XSS уязвимост и потребител случайно последва линк, който се възползва от тази уязвимост, брауърът няма да сподели бисквитката с трета страна.

От друга страна, Secure е опция, която може да бъде зададена от сървъра, когато се изпраща нова бисквитка към потребителя. Флагът на бисквитката Secure предотвратява изпращане на бисквитката по незащитен HTTP (а не по HTTPS) канал. Това на практика добавя едно допълнително ниво на конфиденциалност на бисквитката за разлика от нейния обмен в явен вид.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира изискване за това бисквитките задължително да имат флагове HTTP Only и Secure, като при желание за по-високо ниво на сигурност на системата, е възможно да бъдат включени и допълнителни флагове, като например SameSite. Ако тези изисквания са вече изпълнени от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които няма функционалност за перманентност на връзката посредством технологията бисквитки или други случаи, в които бисквитки не се използват. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

#### **11. Предвидени и предприети ли са мерки за защита на DNS, като задължително се прилага DNSSEC (Domain Name System Security Extensions);**

DNS е една от най-важните системи фасилитираща комуникацията между различните участници в Интернет. За съжаление, сам по себе си DNS не е сигурен, като за да се добави допълнително ниво на сигурност в DNS се използват разширенията DNS. Тези допълнителни разширения добавят две важни характеристики по отношение на сигурността: удостоверяване на произхода на данните; и защита на целостта на данните.

За изпълнение на настоящата точка, изискването за DNSSEC трябва да фигурира в техническата спецификация. Ако тези изисквания са вече изпълнени от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Случаите, в които тази точка може да бъде разглеждана като НЕПРИЛОЖИМА, са например тези, в които системата не се достъпва през Интернет. Причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

**12. По отношение на системните записи (Logs) предвидени ли са следните възможности:**

- а. в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори да се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;**
- б. за всяко от тези събития в записите да се отбелязва с астрономическото време, когато е настъпило събитието;**
- в. предвидена ли е възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи, като се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time) или аналогичен.**
- г. предвидено ли е информацията да бъде архивирана за срок не по-кратък от дванадесет месеца.**

Системните записи имат изключително важна роля както за верифициране на надеждността на съществуващите контроли за мрежова и информационна сигурност, така и за извършване на разследващо-криминалистична дейност при възникването на сериозни инциденти в мрежовата и информационната сигурност. Те могат да се разглеждат като най-надежден източник на информация за това, какво точно се е случило и да спомогнат за предотвратяване на последващи пробиви в сигурност и по-високо ниво на МИС. За да бъде постигната подобна функционалност, системните записи трябва да отразяват поне изброените в изискването по чл. 29 т. 1 от НМИМИС атрибути, изискването за време и синхронизация по т. 2 и т. 3, както и минималното време за архивиране по т.5, което е 12 месеца.

За изпълнение на настоящата точка, в техническата спецификация следва да фигурира всички гореспоменати изисквания към системните логове и атрибутите които те отразяват. Ако тези изисквания са вече изпълнени от съществуваща архитектура, то това обстоятелство следва да бъде описано ясно, конкретно и в пълен обем.

Не се предвиждат случаи, в които тази точка да бъде НЕПРИЛОЖИМА за определена техническа спецификация. Ако в процеса на работа подобен случай възникне, причините за неприложимостта на настоящото изискване следва да бъдат обосновани ясно, конкретно и в пълен обем в техническата спецификация.

---