Приложение № 1

към чл. 38, ал. 3

Държавна агенция „Електронно управление“

ТЕХНИЧЕСКО ЗАДАНИЕ

за

*НАДГРАЖДАНЕ НА ПОРТАЛА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА НАЦИОНАЛНИЯТ ЦЕНТЪР ЗА РЕАКЦИЯ ПРИ ИНЦИДЕНТИ ВЪВ ВРЪЗКА С ИНФОРМАЦИОННАТА СИГУРНОСТ С ДОПЪЛНИТЕЛНИ ФУНКЦИОНАЛНОСТ*И

СЪДЪРЖАНИЕ

[1 РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ 5](#_Toc494119450)

[1.1 Използвани акроними 5](#_Toc494119451)

[1.2 Използвана терминология 5](#_Toc494119452)

[1.3 Дефиниции за нива на електронизация на услугите 7](#_Toc494119453)

[2 ВЪВЕДЕНИЕ 8](#_Toc494119454)

[2.1 Цел на документа 8](#_Toc494119455)

[2.2 За възложителя – функции и структура 8](#_Toc494119456)

[2.3 За проекта 10](#_Toc494119457)

[2.4 Нормативна рамка 10](#_Toc494119458)

[3 Цели, обхват и очаквани резултати от изпълнение на проекта 10](#_Toc494119459)

[3.1 Общи и специфични цели на проекта 10](#_Toc494119460)

[3.2 Обхват на проекта 11](#_Toc494119461)

[3.3 Целеви групи 11](#_Toc494119462)

[3.4 Очаквани резултати 11](#_Toc494119463)

[3.5 Период на изпълнение 11](#_Toc494119464)

[4 ТЕКУЩО СЪСТОЯНИЕ 11](#_Toc494119465)

[4.1 Функционалност на ядрото (вътрешни модули) на портала 11](#_Toc494119466)

[4.1.1 Модул „Уязвимости“ 12](#_Toc494119467)

[4.1.2 Модул „Конституенти“ 12](#_Toc494119468)

[4.1.3 Модул „Инциденти“ 12](#_Toc494119469)

[4.1.4 Модулите „Участници“, „Партньори“ и „Интернет доставчици“ 13](#_Toc494119470)

[4.1.5 Административен модул 13](#_Toc494119471)

[4.2 Функционалност на административна информационна система и приложение за предоставяне на електронни административни услуги 13](#_Toc494119472)

[4.2.1 Административна информационна система 13](#_Toc494119473)

[4.2.2 Електронни административни услуги 13](#_Toc494119474)

[4.3 Функционалност на публична част на портал за мрежова и информационна сигурност на Националният Център за Реакция при Инциденти във Връзка с Информационната Сигурност (CERT България) 14](#_Toc494119475)

[4.3.1 Система за управление на съдържание 14](#_Toc494119476)

[4.4 Базов софтуер и технология 14](#_Toc494119477)

[5 ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА 15](#_Toc494119478)

[5.1 Общи изисквания към изпълнението на обществената поръчка 15](#_Toc494119479)

[5.2 Общи организационни принципи 15](#_Toc494119480)

[5.3 Управление на проекта 15](#_Toc494119481)

[5.4 Управление на риска 16](#_Toc494119482)

[6 ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА 16](#_Toc494119483)

[6.1 Анализ на данните и изискванията 18](#_Toc494119484)

[6.1.1 Специфични изисквания към етапите на бизнес анализа и разработка 18](#_Toc494119485)

[6.1.2 Специфични изисквания при оптимизиране на процесите по заявяване на електронни административни услуги в зависимост от заявителя 18](#_Toc494119486)

[6.1.3 Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила 18](#_Toc494119487)

[6.1.4 Изисквания към регистрите и предоставянето на административните услуги 19](#_Toc494119488)

[6.2 Изготвяне на системен проект 19](#_Toc494119489)

[6.3 Разработване на софтуерното решение 19](#_Toc494119490)

[6.4 Тестване 19](#_Toc494119491)

[6.5 Внедряване 19](#_Toc494119492)

[6.6 Обучение 20](#_Toc494119493)

[6.7 Гаранционна поддръжка 20](#_Toc494119494)

[7 ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ 21](#_Toc494119495)

[7.1 Функционални изисквания към информационната система 21](#_Toc494119496)

[7.1.1 Интеграция с външни информационни системи 21](#_Toc494119497)

[За реализиране на основни бизнес процеси Системата трябва да поддържа интеграция в реално време с други информационни системи на администрацията. 21](#_Toc494119498)

[7.1.2 Интеграционен слой 21](#_Toc494119499)

[7.1.3 Технически изисквания към интерфейсите 22](#_Toc494119500)

[7.1.4 Електронна идентификация на потребителите 23](#_Toc494119501)

[7.1.5 Отворени данни 23](#_Toc494119502)

[7.1.6 Формиране на изгледи 23](#_Toc494119503)

[7.1.7 Администриране на Системата 23](#_Toc494119504)

[7.2 Нефункционални изисквания към информационната система 23](#_Toc494119505)

[7.2.1 Авторски права и изходен код 23](#_Toc494119506)

[7.2.2 Системна и приложна архитектура 23](#_Toc494119507)

[7.2.3 Повторно използване (преизползване) на ресурси и готови разработки 25](#_Toc494119508)

[7.2.4 Изграждане и поддръжка на множество среди 26](#_Toc494119509)

[7.2.5 Процес на разработка, тестване и разгръщане 26](#_Toc494119510)

[7.2.6 Подписване на документи 26](#_Toc494119511)

[7.2.7 Бързодействие и мащабируемост 27](#_Toc494119512)

[7.2.8 Информационна сигурност и интегритет на данните 28](#_Toc494119513)

[7.2.9 Използваемост 29](#_Toc494119514)

[7.2.10 Системен журнал 30](#_Toc494119515)

[8 ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА 31](#_Toc494119516)

[8.1 Функционален обхват на софтуерните разработки 31](#_Toc494119517)

[8.2 Разширяване на функционалния обхват на портала за мрежова и информационна сигурност 31](#_Toc494119518)

[8.3 Разработване на модул за обработване на постъпващи външни заявки и доклади 31](#_Toc494119519)

[8.4 Добавяне на нови функционалности и доработка на съществуващи в модул „Инциденти“ 32](#_Toc494119520)

[8.4.1 Разработване на типови шаблони за инциденти в модул „Инциденти“ 32](#_Toc494119521)

[8.4.2 Автоматична обработка едновременно на множество IP адреси на засегнати системи 32](#_Toc494119522)

[8.4.3 Модифициране на „Хронология“ 33](#_Toc494119523)

[8.4.4 Модифициране на информацията в някои от екраните / отделните менюта 33](#_Toc494119524)

[8.4.5 Оптимизация на форми, редизайн 33](#_Toc494119525)

[8.5 Преструктуриране на интерфейса за наливане на уязвимости в портала, модул „Уязвимости“ 34](#_Toc494119526)

[8.5.1 Адаптиране към обновената структура на данните в CVE списъците (Common Vulnerabilities and Exposures List) 34](#_Toc494119527)

[8.6 Доразвиване на функционалността за изпращане на информационни бюлетини 34](#_Toc494119528)

[8.7 Доразвиване на функционалността „Сортиране по колони“ 34](#_Toc494119529)

[8.8 Оптимизиране на формата за докладване на инциденти 35](#_Toc494119530)

[8.9 Осигуряване на връзка с изграждащия се Регистър на информационни активи 35](#_Toc494119531)

[8.10 Подобряване на бързодействието на системата 36](#_Toc494119532)

[8.11 Справочна система - Разработка на генератор на справки и отчети 36](#_Toc494119533)

[8.12 Обновяване дизайна на публичната част на портала за МИС www.govcert.bg 37](#_Toc494119534)

[8.13 Разработване на експлоатационна документация 37](#_Toc494119535)

[9 ДОКУМЕНТАЦИЯ 38](#_Toc494119536)

[9.1 Изисквания към документацията 38](#_Toc494119537)

[9.2 Прозрачност и отчетност 38](#_Toc494119538)

[9.3 Системен проект 38](#_Toc494119539)

[9.4 Техническа документация 39](#_Toc494119540)

[9.5 Протоколи 39](#_Toc494119541)

[9.6 Комуникация и доклади 39](#_Toc494119542)

[9.6.1 Встъпителен доклад 39](#_Toc494119543)

[9.6.2 Междинен доклад 39](#_Toc494119544)

[9.6.3 Окончателен доклад 39](#_Toc494119545)

[10 РЕЗУЛТАТИ 40](#_Toc494119546)

# РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

## Използвани акроними

|  |  |
| --- | --- |
| **Съкращение** | **Описание** |
| ДА ЕУ | Държавна агенция Електронно управление |
| МИС | Мрежова и информационна сигурност |
| ЕНИСА | Европейска агенция за мрежова и информационна сигурност |
| ЗЕУ | Закон за електронното управление |
| ЗЕИ | Закона за електронната идентификация |
| ЗЕС | Закона за електронните съобщения |
| CERT Bulgaria | Център за реакции при инциденти във връзка с информационната сигурност |
| АИС | Административна информационна система |
| ПЗОУ | Приложения за заявяване и отговор по услуги |
| NVD | National Vulnerability Database |
| ЕАУ | Електронна административна услуга |
| ISP | Internet Service Provider / Интернет доставчик |
| CVE | Common Vulnerabilitries and Exposures |

## Използвана терминология

| **Термин**  | **Описание**  |
| --- | --- |
| **Виртуална комуникационна инфраструктура**  | Инфраструктура, която на база съществуваща физическа свързаност, предоставена от ДАЕУ, предоставя възможност за изграждане на отделни и защитени виртуални мрежи за всяка една от структурите в сектора, при гарантиране на сигурен и защитен обмен на информация в тях.  |
| **Държавен хибриден частен облак**  | Централизирана на ниво държава информационна инфраструктура (сървъри, средства за съхранение на информация, комуникационно оборудване, съпътстващо оборудване, разпределени в няколко локации, в помещения отговарящи на критериите за изграждане на защитени центрове за данни), която предоставя физически и виртуални ресурси за ползване и администриране от секторите и структурите, които имат достъп до тях, в зависимост от нуждите им, при гарантиране на високо ниво на сигурност, надеждност, изолация на отделните ползватели и невъзможност от намеса в работоспособността на информационните им системи или неоторизиран достъп до информационните им ресурси. Изолацията на ресурсите и мрежите на отделните секторни ползватели (е-Общини, е-Правосъдие, е-Здравеопазване, е-Полиция) се гарантира с подходящи мерки на логическо ниво (формиране на отделни клъстери, виртуални информационни центрове и мрежи) и на физическо ниво (клетки и шкафове с контрол на достъпа).  |
| **Софтуер с отворен код**  | Компютърна програма, която се разпространява при условия, които осигуряват безплатен достъп до програмния код и позволяват: Използването на програмата и производните на нея компютърни програми, без ограничения в целта; Промени в програмния код и адаптирането на компютърната програма за нуждите на нейните ползватели; Разпространението на производните компютърни програми при същите условия. Списък на стандартни лицензионни споразумения, които предоставят тези възможности, който може да бъде намерен в подзаконовата нормативна уредба към Закона за електронно управление или на: <http://opensource.org/licenses>. |
| **Машинно четим формат**  | Формат на данни, който е структуриран по начин, по който, без да се преобразува в друг формат позволява софтуерни приложения да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура.  |
| **Отворен формат**  | Означава формат на данни, който не налага употребата на специфична платформа или специфичен софтуер за повторната употреба на съдържанието и е предоставен на обществеността без ограничения, които биха възпрепятствали повторното използване на информация.  |
| **Метаданни**  | Данни, описващи структурата на информацията, предмет на повторно използване.  |
| **Официален отворен** **стандарт**  | Стандарт, който е установен в писмена форма и описва спецификациите за изискванията как да се осигури софтуерна оперативна съвместимост.  |
| **Система за контрол на версиите**  | Технология, с която се създава специално място, наречено “хранилище”, където е възможно да се следят и описват промените по дадено съдържание (текст, програмен код, двоични файлове). Една система за контрол на версиите трябва да може: * Да съхранява пълна история - кой, какво и кога е променил по съдържанието в хранилището, както и защо се прави промяната;
* Да позволява преглеждане разликите между всеки две съхранени версии в хранилището;
* Да позволява при необходимост съдържанието в хранилището да може да се върне към предишна съхранена версия;
* Да позволява наличието на множество копия на хранилището и синхронизация между тях.

Цялата информация, налична в системата за контрол на версиите за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, трябва да може да бъде достъпна публично, онлайн, в реално време.  |
| **Първичен регистър**  | Регистър, който се поддържа от първичен администратор на данни - административен орган, който по силата на закон събира или създава данни за субекти (граждани или организации) или за обекти (движими и недвижими) за първи път и изменя или заличава тези данни. Например Търговският регистър е първичен регистър за юридическите лица със стопанска цел, Имотният регистър е първичен регистър за недвижима собственост.  |
| **СУСИ** | Система за управление на сигурността на информацията съгласно изискванията на БДС ISO/IEC 2700 |
| **Сигурност на информацията** | Запазване на поверителност, цялостност и наличност на информацията, а също така и автентичност, отчетност и надеждност |
| **Събитие, свързано със сигурността на информацията** | Идентифицирана поява на състояние в система, услуга или мрежа, показваща възможно нарушение на политиката по сигурност на информацията, пробив на защити или неизвестна до момента ситуация, засягаща сигурността |
| **Атака**  | Злонамерена дейност, която цели да разруши, да осигури контрол над компютърна среда/инфраструктура, да наруши интегритет на данни или открадне контролирана информация. |
| **Заплаха** | Заплаха е потенциално възможно произшествие, което може да окаже нежелателно въздействие върху самата система, а също така върху информацията, която се съхранява в нея, и не е важно, дали това произшествие е преднамерено или не е |
| **Конституент** | Клиент (ползвател на услугите) на CSIRT / CERT, съгласно дефинициите на ENISA |
| **Инцидент** | Всяко спиране на портала и/или негов компонент, както и изменение в тяхната работоспособност или получаване на неочаквани резултати (забавяне на достъпа, забавяне в опресняването на екраните, визуализиране на нестандартни/ неочаквани съобщения, и т.н.) |
| **Време за възстановяване** | Времето от момента на регистриране на инцидента до момента на неговото затваряне (възстановяване на нормалната работа на Портала) |
| **Време за реакция** | Времето от момента на регистриране на заявката до момента на започване на работа по нея. |
| **Проблем** | Първопричина за един или повече инцидента, която е известна |
| **Класификация** | Въз основа на обща характеристика на инциденти, по която може да се групират и да се търси първопричината за възникването им |
| **Приоритет** | Базира се на възможния ефект който може да окаже инцидента или на спешността на действията, които трябва да се извършат за отстраняването му и се използва за дефиниране на времена за реакция от обслужващите екипи с цел своевременно извършване на необходимите дейности |

## Дефиниции за нива на електронизация на услугите

| **Термин**  | **Описание**  |
| --- | --- |
| **Ниво 1**  | Информация - предоставяне на информация за административни услуги по електронен път, включително за начини и места за заявяване на услугите, срокове и такси. |
| **Ниво 2**  | Едностранна комуникация - информация съгласно дефиницията за Ниво 1 и осигурен публичен онлайн достъп до шаблони на електронни формуляри. |
| **Ниво 3**  | Двустранна комуникация - заявяване и получаване на услуги изцяло по електронен път, включително електронно подаване на данни и документи, електронна обработка на формуляри и електронна персонална идентификация на потребителите. |
| **Ниво 4**  | Извършване на сделки или транзакции по услуги от Ниво 3, включващи онлайн разплащане или доставка. |

# ВЪВЕДЕНИЕ

## Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на обществена поръчка с предмет: *Надграждане на портала за мрежова и информационна сигурност на Националният център за реакция при инциденти във връзка с информационната сигурност с допълнителни функционалности*.

В настоящото техническо задание са описани и изискванията към проектната организация, документацията и отчетността.

## За възложителя – функции и структура

Държавна агенция „Електронно управление“ (ДАЕУ) към Министерския съвет е създадена със Закона за електронното управление (обн. ДВ, бр. 50 от 2016 г.). Агенцията е юридическо лице на бюджетна издръжка със седалище в гр. София. Председателят на ДА „Електронно управление“ е първостепенен разпоредител с бюджет, определя се с Решение на Министерския съвет и се назначава от министър-председателя за срок от 5 години.

Агенцията е правоприемник на дирекция „Електронно управление” в Министерството на транспорта, информационните технологии и съобщенията и на Изпълнителната агенция „Електронни съобщителни мрежи и информационни системи”.

Структурата на *Държавна агенция „Електронно управление“* е представена във Фигура1:



Фигура 1. Структура на *ДА ЕУ*

Държавна агенция „Електронно управление” има функции по издаване, налагане и контрол на политики, правила и добри практики в областта на електронното управление, стратегическо планиране и инициативи, бюджетно програмиране и контрол, координация на секторни политики и секторни и междуведомствени проекти. Агенцията ще поддържа също така централизирани регистри за нуждите на електронното управление, други централизирани регистри, държавен частен облак и комуникационната мрежа на държавната администрация.

Председателят на ДАЕУ провежда държавната политика в следните области:

* Електронно управление;
* Електронни удостоверителни услуги;
* Електронна идентификация;
* Мрежова и информационна сигурност;
* Инфраструктура за пространствена информация;
* Информация от обществения сектор в машинночетим отворен формат.

При осъществяването на държавната политика в посочените области председателят на агенцията изпълнява правомощия, възложени му със Закона за електронното управление (ЗЕУ), Закона за електронната идентификация (ЗЕИ), Закона за електронните съобщения (ЗЕС), други закони или с акт на Министерския съвет.

Важно функционално звено от ДА ЕУ е Център за реакции при инциденти във връзка с информационната сигурност (CERT Bulgaria), който има национален статут.

Мисията на Центъра е да подпомага ползвателите на услугите му в извършване на проактивни дейности за намаляване рисковете от инциденти в информационната сигурност и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали.

Конституенти на Център за реакции при инциденти във връзка с информационната сигурност са органите на държавната власт, органите на местното самоуправление и юридическите лица, разпоредители с бюджетни кредити.

Отговорността за информационната сигурност става все по-важна поради увеличаващия се брой заплахи и активирането на кибер престъпността в световен мащаб.

Способността за бърза и ефективна реакция на атаки и заплахи към сигурността на информацията е изключително критична за нормалното функциониране на администрацията.

Задачите, които изпълнява Националния център за реакции при инциденти във връзка с информационната сигурност са в съответствие с методическите указания с на Европейската агенция за мрежова и информационна сигурност (ENISA), както и с добрите европейски и световни практики в областта на информационната сигурност и включват, като част от тях са:

* популяризиране на проактивни мерки за защита на информацията и технологичните активи;
* своевременно информиране за уязвимости и заплахи;
* реагиране на инциденти в мрежовата и информационната сигурност;
* оценяване въздействието на инциденти в мрежовата и информационната сигурност;
* оказване на помощ при възстановяване след инциденти;

Голяма част от тези задачи Националния център за реакции при инциденти във връзка с информационната сигурност изпълнява чрез портала за мрежова и информационна сигурност govcert.bg.

Достъпността и правилното функциониране на портала са един от основните критерии за ефективното функциониране на Националния център за реакции при инциденти във връзка с информационната сигурност, а също така е и едно от основните изисквания на Trusted Introducer, която е международна организация акредитирана за сертифициране на Национални CERTs.

## За проекта

Въпреки обновяването на информационната система, с която работи Националният център за реакция при инциденти в информационната сигурност, при изпълнение на проект „Подобряване на административното обслужване на потребителите чрез надграждане на централните системи на електронното правителство” с рег. № К11-32-1/ 20.09.2011г., осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет”, за постигане на пълнота и цялостност на единната информационно-комуникационна среда е необходимо да се разработят допълнителни функционалности и интеграционни компоненти.

От друга страна, въз основа на натрупания опит от реалната експлоатация на системата – както от страна на служителите на ведомството, така и от страна на външните потребители на неговите услуги, са идентифицирани нови потребности от по-нататъшното му надграждане и развитие, осигурявайки приемственост и допълняемост между отделните проекти.

Не на последно място, за да се гарантира достатъчно продължителен период на жизненост на една система, тя се нуждае от непрекъснати подобрения, които трябва да отразяват непрекъснато променящите се реалности в правния мир, обществено-икономическия живот и динамиката на развитие на технологиите.

В този контекст, един 4-годишен период от формулирането на изискванията към сегашната информационно-комуникационна среда, е достатъчно дълъг период за натрупване на опит и изготвяне на реалистична оценка, относно нуждите от нейната актуализация и изпълнение на следваща стъпка от нейното развитие, в резултат на което е инициирана настоящата поръчка.

## Нормативна рамка

* Закон за електронното управление
* Правилник за дейността, структурата и организацията на Държавна агенция „Електронно управление“
* Закона за електронната идентификация
* Закона за електронните съобщения
* Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги
* Наредба за общите изисквания за мрежова и информационна сигурност
* Наредба за електронните административни услуги
* Наредба за обмена на документи в администрацията
* Наредба за удостоверенията за електронен подпис в администрациите
* Наредба за стандартните условия за повторно използване на информация от обществения сектор и за нейното публикуване в отворен формат

# Цели, обхват и очаквани резултати от изпълнение на проекта

## Общи и специфични цели на проекта

Целите на поръчката са подчинени на общата цел на агенцията непрекъснато да подобрява качеството на своята работа и на предоставяните услуги за нашите конституенти. Един от основните инструменти за постигане на тази цел е внедряването на нови и непрекъснатото усъвършенстване на съществуващите информационни технологии в агенцията. Това е в пълно съответствие със стратегическите цели на правителството по отношение на административното обслужване и въвеждането на електронното управление.

Чрез реализацията на новите функционалности се цели:

* Намаляване на ръчната обработка на данни и минимизиране на възможността за грешки и пропуск.
* Осигуряване на възможност за генериране и извличане на разнообразна справочна и статистическа информация въз основа на натрупаните данни.
* Автоматизиране процеса на генериране на дневни отчети за обработените инциденти.
* Увеличаване на работоспособността и повишаване качеството на обслужване чрез намаляване времето за обработка и разрешаване на инциденти.

## Обхват на проекта

Описаните в т. 3.1 цели се осъществяват с изпълнението на настоящата поръчка за „Надграждане с допълнителни функционалности на Портала за мрежова и информационна сигурност на Националният център за реакция при инциденти във връзка с информационната сигурност“.

Поръчката обхваща анализ, проектиране, разработване, тестване, внедряване и поддръжка на нови и доразвиване на съществуващи функционалности, както и обучение на ключови потребители и администратори за работа с тях.

## Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

* *Централна администрация*;
* *Местна администрация*;
* *Интернет доставчици*

## Очаквани резултати

Очакваните резултати от изпълнението на настоящата поръчка са:

* *Автоматизиране на процеса на управление на инциденти*;
* *Нова визия на Националния портал за МИС*;
* *Автоматизиране на процеса на генериране на отчети, справки и статистика.*

## Период на изпълнение

Периодът на изпълнение на поръчката е четири месеца от датата на сключване на договор

Участниците трябва да изготвят подробен график, в който следва да се конкретизират сроковете за изпълнение на всяка дейност и поддейност от настоящата поръчка. Графикът за изпълнение трябва да бъде съобразен с продължителността на дейността и не може да надвишава *4 (четири)* месеца от дата на сключване на договора.

# ТЕКУЩО СЪСТОЯНИЕ

Порталът за мрежова и информационна сигурност на Националният център за реакция при инциденти във връзка с информационната сигурност (Портал на CERT България) се състои от следните компоненти:

* Ядро (вътрешни модули) на системата;
* Административна информационна система и приложение за предоставяне на електронни административни услуги;
* Публичен портал на Националният център за реакция при инциденти във връзка с информационната сигурност (CERT България).

## Функционалност на ядрото (вътрешни модули) на портала

Ядрото на системата се състои от следните седем модула:

* Уязвимости
* Инциденти
* Участници
* Конституенти
* Партньори
* Интернет доставчици
* Администриране

До вътрешният модул имат достъп само отговорниците по МИС, определени със заповед на ръководителя на съответната администрация. Влизането в системата става чрез потребителско име и парола и за целта не е необходима никаква допълнителна инсталация. Порталът предоставя едновременен достъп на неограничен борй потребители.

### Модул „Уязвимости“

В този модул автоматично се събира и обновява информация за ежедневно публикуваните уязвимости.

За смекчаване на рисковете и намаляване на броя на необходимите действия CERT - България предлага на своите конституенти като превантивни услуги:

* бюлетини за уязвимости в използвания софтуер и хардуер;
* уведомява потребителите за експлойти и вируси, които се възползват от тези недостатъци;
* предлага решения за отстраняването им.

По този начин конституентите могат бързо да реагират на заплахите към сигурността.

### Модул „Конституенти“

Чрез този модул се поддържа необходимата информация за конституентите. Поддържането на информацията се осъществява от:

* конституентът чрез профила си в Портала за мрежова и информационна сигурност;
* CERT – България пряко чрез Портала.

Чрез този модул се събира и съхранява информация за информационната и комуникационна инфраструктура на конституентите на CERT - България. По този начин може да се оценят уязвимостите в ИТ инфраструктурата на конституентите, както и да се прави анализ при взимане на решение в случай на реакция на инцидент. Информацията се използва за филтриране на предупреждения при новооткрити уязвимости, така че конституентите да не са затрупани с информация, която е по същество ненужна за тях.

Конституентите могат да подават и актуализират информацията за собствените си информационни и комуникационни системи чрез профила си в портала за мрежова и информационна сигурност само чрез ЕАУ.

### Модул „Инциденти“

Служи за документиране на действията от процеса на управление на инциденти, което се осъществява ръчно от служител на CERT България.

* Получаване на сигнал: Сигнали за нарушения във и от българското Интернет пространство се получават в CERT - България по няколко канала: електронна поща, като ЕАУ, телефон или факс.
* Класификация на сигнала като инцидент се извършва, съгласно таксономията на Европейската агенция за мрежова и информационна сигурност (ENISA).
* Анализ на информацията: По време на този процес е възможно да се поиска и допълнителна информация, свързана с инцидента;
* Определяне на възможни решение;
* Предложение за действия;
* Предприемане на действия;
* Отстраняване на причините за инцидента и възстановяване на функционалността на засегната система;
* Затваряне на инцидент: Процесът завършва, когато всички засегнати страни са докладвали за възстановяване нормалната работоспособност след справяне с инцидента.
* Архивиране: Събраната в процеса на управление на инцидента информация се архивира съобразно приетите политики за информационна сигурност.

### Модулите „Участници“, „Партньори“ и „Интернет доставчици“

В тези модули се поддържа актуална информация за участниците в инцидентите – като например лица за контакти, емейл адреси, телефони, IP адреси и др.

### Административен модул

Чрез административния модул на системата:

* се подържат конфигурации, параметри и настройки на системата;
* се поддържат базови номенклатури за работата на системата;
* се управляват потребители, права и роли;
* се задават политиките за архивиране на информацията;
* се изпълняват други функции за администриране на системата.

## Функционалност на административна информационна система и приложение за предоставяне на електронни административни услуги

### Административна информационна система

Електронните административни услуги, предоставяни от CERT – България се реализират от Портала на CERT. За целта в нея е изграден модул „АИС”.

Модулът „АИС” осигурява функционалност на административна информационна система (АИС) за електронен документооборот, съгласно Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Основните функции на модул „АИС” са:

* осигурява поддържането и обработката на данните за оборота на електронни документи при предоставянето на административни услуги;
* осигурява поддържането и обработката на данните за оборота на електронни документи при изпълнението на административни процедури (работни процеси в администрацията или между различните администрации, които включват вътрешен оборот на документи и които не представляват предоставяне на административни услуги и вътрешни електронни административни услуги);
* поддържа и осигурява съхранението на приетите и създаваните електронни документи;
* чрез него могат да се създават електронни документи.

### Електронни административни услуги

Чрез Порталът за МИС се предоставят четири ЕАУ:

* Уведомяване на CERT България за инцидент в информационните системи на администрацията;
* Предоставяне на информация на CERT България относно уязвимости, свързани с информационната сигурност;
* Абониране за бюлетин за възможни заплахи и/или възникващи инциденти в информационната сигурност;
* Поддържане на информация за инсталационната база на конституента.

Всички етапи на изпълнение на услугите са унифицирани и са описани подробно в документацията при изграждането на Портала. Заявителят подписва заявлението чрез софтуерен инструмент, предоставен от портала, който му позволява да постави електронния си подпис (намиращ се на софтуерен или хардуерен носител, издаден от Доставчици на доверителни услуги в ЕС, които отговарят на изискванията за унифициран профил на електронните подписи, съгласно подзаконовите правила към Регламент ЕС 910/2014) върху XML документа на заявлението. Заявителят (конституент или партньор) може да преглежда всички подадените от него заявления. За всяко от заявлението може да получи хиперлинк за преглед на детайли, пренасочващ към раздела на официалната преписка в АИС.

За създаване на условия за осъществяване на ЕАУ към портала са разработени:

* Приложения за заявяване и отговор по услуги (ПЗОУ - уеб-базирано приложение) - информационна система, осигуряваща чрез интернет страница или друг електронен интерфейс възможността на изпращане и/или получаване на електронни изявления от и към доставчиците на електронни административни услуги. АИС подлежи на сертификация, съгласно наредбите към ЗЕУ;
* Регистрация и поддръжка на потребителски профил с възможност за съхраняване и използване на информация за използвани услуги;
* Функционалност за проверка на статуса на услуга.

ПЗОУ са напълно съобразени с изискванията на ЗЕУ и подлежат на сертификация. Електронните услуги се изпълняват чрез ПЗОУ и АИС.

## Функционалност на публична част на портал за мрежова и информационна сигурност на Националният Център за Реакция при Инциденти във Връзка с Информационната Сигурност (CERT България)

### Система за управление на съдържание

Чрез публичния портал са достъпни следните електронни административни услуги:

* Уведомяване на CERT България за инцидент в информационните системи на администрацията;
* Предоставяне на информация на CERT България, относно уязвимости, свързани с информационната сигурност;
* Абониране за бюлетин за възможни заплахи и/или възникващи инциденти в компютърната сигурност;
* Поддържане на информация за инсталационната база на конституента.

## Базов софтуер и технология

Порталът за МИС използва следния базов софтуер и технология с отворен код:

* Сървър за приложения – GlassFish Server;
* База данни – MySQL;
* Портален сървър – Liferay Portal;
* Език за програмиране – Java.

Той е инсталиран върху виртуална машина с операционна система Windows Server 2012. За осигуряване на безпроблемната му работа се спазват разработените процедури за ежедневно архивиране на данните на допълнителен SCSI диск и седмично архивиране на виртуалната машина.

# ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

## Общи изисквания към изпълнението на обществената поръчка

Обществената поръчка се изпълнява в рамките на *„Надграждане с допълнителни функционалности на Портала за мрежова и информационна сигурност на Националният център за реакция при инциденти във връзка с информационната сигурност“*, финансиран от бюджета на ДА ЕУ. Изпълнителят следва да спазва всички нормативни изисквания по отношение на дейността на *ДА ЕУ* и електронното управление в Република България.

Участниците трябва да представят в своите предложения **концепция за изпълнение на поръчката,** включваща описание на конкретен подход за реализация на всяка от функционалностите, изложени в под-разделите на настоящия раздел. Предложенията трябва да съдържат техническо описание на предлаганата реализация, със съответна обосновка в конкретния контекст на поръчката. Предлаганите технологии трябва да са съвместими с общата технологична рамка на агенцията, описана в настоящата техническа спецификация.

## Общи организационни принципи

Изисквания към участника:

* Да притежава валиден сертификат по ISO/IEC 20000-1:2012 - Информационни технологии. Управление на услуги. Част 1: Изисквания относно системата за управление на услуги, или еквивалент
* Да притежава валиден сертификат по ISO/IEC 27001:2013 – „Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания“ или еквивалент.

Място на изпълнение:

* Услугите в обхвата на обществената поръчка ще се изпълняват на територията на Република България.
* Инсталациите на доработената система и нови компоненти към нея ще се извърши в помещение на Възложителя.
* Обучението ще се проведе на територията на гр. София в офис на Възложителя.
* Материалите, резултат от изпълнението ще се предават в офис на Възложителя на адреса на Възложителя.

Участникът следва да разпише подробно в своето предложение начините за управление на качеството по време на изпълнение на поръчката на възложителя. Предложението следва да съдържа дейностите за проследяване и контрол на качеството, както и описание на създадената при участника организация за управление на качеството.

Участникът трябва да опише в своето техническо предложение:

* + Система за осигуряване на качеството и контрол – всички етапи, роли и компоненти за осигурява и контрол на качеството;
	+ Процедури за осигуряване на качеството и контрол – описание на основните процеси и стъпки по осигуряване на качеството и контрола;
	+ Процедура за управление на промените, с която да се регламентира начинът, по който ще бъдат подавани евентуални искания за промяна.

## Управление на проекта

Участниците трябва да представят в своите предложения **концепция за изпълнение на поръчката,** включваща описание на:

* избраната от участника **методология за управление на проекти** (напр. PRINCE2, PMBOK, Six Sigma или еквивалентна). Участникът следва да опише предлаганата от него методология за управление на проекта, която да се базира на утвърдени стандарти и добри практики. Под управление на проекта следва да се разбират процесите по планиране и контрол на обхванатите от проекта дейности и ресурси, необходими за реализация му. Участникът трябва да опише:
* Начини за ефективното прилагане на избраната методология с оглед постигане на очакваните резултати;
* Фази на проекта и основни дейности, характерни за всяка фаза;
* Примерен комуникационен план, с който да покаже по какъв начин с какви средства и с каква регулярност се планират комуникациите с възложителя;
* Ползите от прилагането на методологията за управление на проекти в контекста на настоящата поръчка;
* Начините за управление на качеството, съгласно раздел 6 от настоящата техническа спецификация;
* Управление на риска, съгласно раздел 7 от настоящата техническа спецификация.
* Избраната от тях **методология за софтуерна разработка** (RUP, Scrum, DSDM или еквивалентна).

## Управление на риска

Участникът следва да предложи и създаде организация за управление на риска по време на изпълнение на поръчката, съобразно предложената методология за управление на проекта.

Участникът трябва да представи План за управление на риска като част от техническото предложение. Планът трябва да описва подход за идентифициране и оценяване на риска. Възложителят е идентифицирал следните общи рискове и заплахи при изпълнение на проекта:

* + Недостатъчна експертна подкрепа, съдействие и ангажираност от страна на екипа на възложителя;
	+ Липса на информация или недостатъчна информация, необходима за изпълнение на задачите в рамките на поръчката;
	+ Неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на договора;
	+ Липса на сътрудничество между възложител и изпълнител;
	+ Различни цели и очаквания на заинтересованите лица;
	+ Липсата на задълбоченост при изследването и описанието на бизнес процесите, свързани с административните услуги, които следва да бъдат електронизирани;
	+ Промени в изискванията/обхвата по време на изпълнение на поръчката;
	+ Изменения в нормативната уредба, които могат да предизвикат промяна в обхвата на планирани действия или да наложат ограничителни мерки.

# ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

В техническото си предложение участниците трябва да предложат подход за изпълнение на проекта, като включат минимум следните етапи:

| **Етап** | **Резултати** | **Срок** |
| --- | --- | --- |
| Етап 1: Анализ и проектиране | * График за изпълнение
 | До 10 работни дни след сключване на договор |
| * Спецификация на софтуерните изисквания;
* Техническа спецификация;
 | До 1 месец след сключване на договор |
| Етап 2: Разработка и внедряване | * Пълен програмен код на разработените в обхвата на поръчката функционалности;
* Тестови случаи за приемни тестове на новите функционалности;
* Документация за разработените в обхвата на поръчката модули и функционалности:
	+ Ръководство за потребителя;
	+ Ръководство за администратора
	+ Описание на използваните полета в базата.
* Разработени нови функционалности – в изпълним и инсталационен вид, вкл. инструкции за инсталация и скриптове за създаване на обекти в базата данни;
* Доставени лицензи за стандартен софтуер (в случай, че Изпълнителят е предложил такъв);
* Предоставяне на всички пароли за достъп (административни и дизайнерски);
* Обучение за работа и администриране на надградената система.
 | До 3 месеца след сключване на договор |
| Етап 3: Поддръжка | * Извършване на дейностите по гаранционно обслужване – отстраняване на грешки и неизправности в работата на портала, отстраняване на пропуски в реализацията на функционалностите, описани и залегнали в детайлната техническа спецификация, приета от Възложителя.
 | 1 г. след подписване на окончателен приемо-предавателен протокол |

**Дейности в обхвата на Етап 1: Анализ и проектиране:**

В началото на изпълнението на етапа Изпълнителят трябва да изготви детайлен график за изпълнение на поръчката, който да съгласува с Възложителя.

Изпълнителят трябва да направи детайлно проучване на изискванията към новите функционалности на системата. Изпълнителят трябва да подготви подробна Спецификация на софтуерните изисквания.

На основа на спецификациите на изискванията, изготвени при анализа, Изпълнителят трябва да проектира новите модули и функционалности и да изготви техническа спецификация.

Спецификацията на софтуерните изисквания и системната архитектура трябва да съдържат структурирани изисквания и модели.

Изпълнителят, въз основа на анализа и софтуерните спецификации, трябва да изготви подробен технически проект за изпълнение на софтуерните разработки, включени в описания в настоящата техническа спецификация функционален обхват.

**Дейности в обхвата на Етап 2: Разработка и внедряване:**

При изграждането на новите модули и функционалности, Изпълнителят трябва да прилага итеративен подход.

На основа на спецификациите на изискванията и на съгласуваните елементи от дизайна, описани по-горе, Изпълнителят трябва да реализира новите модули и функционалности на системата.

Изпълнителят създава специализирани изгледи на данните за справочни цели, инсталира и конфигурира справочната система и конфигурира примерни справки.

Изпълнителят трябва да подготви тестови случаи за приемане на разработената функционалност, съобразени с одобрената от Възложителя спецификация на изискванията.

Новите модули и функционалности трябва да се инсталират, настроят и тестват първо в тестова среда и след отстраняване на грешките да бъдат прехвърлени в продукционна среда.

Трябва да се въведат всички номенклатури, класификатори и конфигурации (ако е необходимо въвеждането на такива).

Трябва да се внедри и интегрира модулът за обработка на външни заявки и доклади с портала за мрежова и информационна сигурност.

Трябва да се проиграят всички разработени процедури и инструкции.

Трябва да се изготвят ръководства за администраторите и потребителите на системата.

Трябва да се предаде изходния програмен код на разработения софтуер с необходимите разяснения и техническа документация съдържаща описание и конфигурации.

Трябва да бъдат проведени обученията за работа с новите модули и функционалности на минимум пет ключови потребителя и двама администратора на системата. Обучението трябва да се извърши с готовата за внедряване система. Продължителността на обучението е минимум един работен ден.

В този етап трябва да бъдат доставени лицензи за допълнителен базов софтуер, ако Изпълнителят е предложил такъв.

В рамките на фазата на внедряване Изпълнителят трябва да интегрира всички компоненти на предлаганото решение с изградената и действаща система.

## Анализ на данните и изискванията

В началото на изпълнението на етап 1, Изпълнителят трябва да изготви детайлен график за изпълнение на поръчката, който да съгласува с Възложителя.

Изпълнителят трябва да направи детайлно проучване на изискванията към новите функционалности на системата. Изпълнителят трябва да подготви подробна Спецификация на софтуерните изисквания.

### Специфични изисквания към етапите на бизнес анализа и разработка

На основа на спецификациите на изискванията, изготвени при анализа, Изпълнителят трябва да проектира новите модули и функционалности и да изготви техническа спецификация.

Спецификацията на софтуерните изисквания и системната архитектура трябва да съдържат структурирани изисквания и модели.

### Специфични изисквания при оптимизиране на процесите по заявяване на електронни административни услуги в зависимост от заявителя

*Неприложимо*

### Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила

*Неприложимо*

### Изисквания към регистрите и предоставянето на административните услуги

*Неприложимо*

## Изготвяне на системен проект

Изпълнителят, въз основа на анализа и софтуерните спецификации, трябва да изготви подробен системен проект за изпълнение на софтуерните разработки, включени в описания в настоящата техническа спецификация функционален обхват.

Системният проект подлежи на одобрение от Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в системния проект в срок не по-късно от *5* работни дни.

## Разработване на софтуерното решение

При изграждането на новите модули и функционалности, Изпълнителят трябва да прилага итеративен подход.

На основа на спецификациите на изискванията и на съгласуваните елементи от дизайна, описани по-горе, Изпълнителят трябва да реализира новите модули и функционалности на системата.

Изпълнителят създава специализирани изгледи на данните за справочни цели, инсталира и конфигурира справочната система и конфигурира примерни справки.

Изпълнителят трябва да подготви тестови случаи за приемане на разработената функционалност, съобразени с одобрената от Възложителя спецификация на изискванията.

Новите модули и функционалности трябва да се инсталират, настроят и тестват първо в тестова среда и след отстраняване на грешките да бъдат прехвърлени в продукционна среда.

Трябва да се въведат всички номенклатури, класификатори и конфигурации (ако е необходимо въвеждането на такива).

## Тестване

Изпълнителят трябва да проведе тестване на софтуерното решение в създадена за целта тестова среда, за да демонстрира, че изискванията са изпълнени. Изпълнителят трябва да предложи и опише методология за тестване, която ще използва в план за тестване с описание на обхвата на тестването, вид и спецификация на тестовете, управление на дефектите, регресионна политика, инструменти, логистично осигуряване и други параметри на процеса.

## Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда на *ДА ЕУ.* Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда на *ДА ЕУ*

Трябва да се внедри и интегрира модулът за обработка на външни заявки и доклади с портала за мрежова и информационна сигурност.

Трябва да се проиграят всички разработени процедури и инструкции.

Трябва да се изготвят ръководства за администраторите и потребителите на системата.

Трябва да се предаде изходния програмен код на разработения софтуер с необходимите разяснения и техническа документация съдържаща описание и конфигурации.

В този етап трябва да бъдат доставени лицензи за допълнителен базов софтуер, ако Изпълнителят е предложил такъв.

В рамките на фазата на внедряване Изпълнителят трябва да интегрира всички компоненти на предлаганото решение с изградената и действаща система.

## Обучение

Трябва да бъдат проведени обученията за работа с новите модули и функционалности на минимум пет ключови потребителя и двама администратора на системата. Обучението трябва да се извърши с готовата за внедряване система. Продължителността на обучението е минимум един работен ден.

## Гаранционна поддръжка

Периодът на гаранционната поддръжка да бъде минимум една година след приемане на разработката и да се използва online система за регистриране и проследяване на заявката.

За целта да бъде подробно разработена процедура за гаранционно обслужване, която да съдържа:

* Срок на гаранционната поддръжка
* Обхват на гаранционната поддръжка
* Организация на поддръжката
* Дейности по поддръжката
* Методология за извършване на поддръжката
* Система за проследяване и регистриране на инциденти

Гаранционното поддържане започва да тече от деня на подписване на окончателния приемо-предавателен протокол.

Гаранционната поддръжка трябва да включва минимум следното:

* Отстраняване на всички установени от възложителя несъответствия при функционирането на модулите с изискванията на техническата спецификация;
* Извършване на диагностика на докладван проблем с цел осигуряване на правилното функциониране на системите и модулите;
* Отстраняване на дефектите, открити в софтуерните модули, които са модифицирани или разработени в обхвата на проекта;
* Консултации за разрешаване на проблеми по предложената от Изпълнителя конфигурация на средата (операционна система, база данни, middleware, хардуер и мрежи), използвана от приложението, включително промени в конфигурацията на софтуерната инфраструктура на мястото на инсталация;
* Възстановяването на системата и данните при евентуален срив на системата, както и коригирането им в следствие на грешки в системата;
* Експертни консултации по телефон и електронна поща за системните администратори на Възложителя за идентифициране на дефекти или грешки в софтуера;
* Актуализация и предаване на нова версия на документацията на системата при установени явни несъответствия с фактически реализираните функционалности, както и в случаите, в които са извършени действия по отстраняване на дефекти и грешки, в рамките на гаранционната поддръжка.

# ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

## Функционални изисквания към информационната система

### Интеграция с външни информационни системи

## За реализиране на основни бизнес процеси Системата трябва да поддържа интеграция в реално време с други информационни системи на администрацията.

Да се реализира автоматизиран онлайн обмен на данни между изграждащия се Регистър на информационни активи и Портала за мрежова и информационна сигурност на Република България, чрез идентификация на информационните активите съгласно National Institute of Standards and Technology (NIST) - Common Platform Enumeration (СРЕ) (https://scap.nist.gov/specifications/cpe/), за обобщени данни подробно уточнени в етапа на анализ, описани в софтуерна спецификация.

Минималните обобщени данни за конкретна административна структура (Наименование, Тип, Подтип, ЕИК) са описани по-долу:

1. Обобщени данни за обща софтуерна инсталационна база – операционни системи и приложни софтуери по вид:
	* Статус на софтуера;
	* Тип/Вид на софтуера.
2. Обобщени данни за мрежово оборудване:
	* Статус на хардуера;
	* Тип/Вид на мрежовото оборудване;
	* Тип IP address;
	* IP address.
3. Обобщени данни за сървърно оборудване:
	* Статус на сървърното оборудване;
	* Тип/Вид на софтуера;
	* Роля на сървъра;
	* Тип/вид на машината (или виртуална);
	* Тип IP address;
	* IP address.
4. Обобщени данни за публични мрежови адреси:
	* Данни за начален и краен IP адрес от обхвата;
	* Указване на повече от един обхват от IP адреси.

### Интеграционен слой

Приложението трябва да се реализира чрез стандартен интеграционен слой като вътрешна услуга (service).

Трябва да бъде разработен и внедрен служебен онлайн интерфейс за машинен обмен на данни и предоставяне на вътрешноадминистративни електронни услуги към информационни системи и регистри на други администрации, публични институции и доставчици на обществени услуги, съгласно действащите изисквания за оперативна съвместимост. Трябва да бъде предвидена интеграция с първични регистри чрез стандартен междинен слой или чрез националната схема за електронна идентификация – конкретната реализация трябва да бъде одобрена от Възложителя след приключване на етапа на бизнес-анализ.

Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на документи и нотификации чрез електронна препоръчана поща към подсистемата за сигурно връчване, част от Националната система за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост.

Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на транзакционна история към системата за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост.



### Технически изисквания към интерфейсите

Приложните програмни интерфейси трябва да отговарят на следните архитектурни, функционални и технологични изисквания:

* Служебните онлайн интерфейси трябва да се предоставят като уеб-услуги (web-services) и да осигуряват достатъчна мащабируемост и производителност за обслужване на синхронни заявки (sync pull) в реално време, с максимално време за отговор на заявки под 1 секунда за 95% от заявките, които не включват запитвания до регистри и външни системи. Изпълнителят трябва да обоснове прогнозирано натоварване на Системата и да предложи критерии за оценка на максимално допустимото време за отговор на машинна заявка. Критерият за оценка следва да се основава на анализ на прогнозираното натоварване и на наличния хардуер, който ще се използва. Изпълнителят трябва да представи обосновано предложение за минималното време за отговор на заявка на базата на посочените по-горе критерии и да осигури нужните условия за спазването му;
* Всички публични и служебни онлайн интерфейси трябва да бъдат реализирани с поддръжка на режими “push” и „pull”, в асинхронен и синхронен вариант – практическото прилагане на всяка от комбинациите трябва да бъде определено на етап бизнес-анализ и да бъдат съобразени реалните казуси (use cases), които всеки интерфейс обслужва;
* Да бъде предвидено създаването и поддържането на тестова среда, достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или за бизнеса, с цел по-лесно и устойчиво интегриране на съществуващите и бъдещи информационни системи.

### Електронна идентификация на потребителите

Електронната идентификация трябва да се реализира чрез интеграция на разработения за нуждите на електронното управление пилотен приложен модул е-автентикация, собственост на ДА ЕУ.

### Отворени данни

*Неприложимо на основание Приложение 1 към чл. 25 от ЗЗКИ.*

### Формиране на изгледи

Потребителите на Системата трябва да получават разрези на информацията чрез филтриране, пренареждане и агрегиране на данните. Резултатът се представя чрез:

* Визуализиране на таблици;
* Графична визуализация на екран;
* Разпечатване на хартиен носител;
* Експорт на данни в един или в няколко от изброените формати – ODF, Excel, PDF, HTML, TXT, XML, CSV.

### Администриране на Системата

Системата трябва да осигурява администриране на потребителите и правата за достъп.

## Нефункционални изисквания към информационната система

### Авторски права и изходен код

Всички компютърни програми, които се разработват за реализиране на Системата, трябва да отговарят на критериите и изискванията за софтуер с отворен код;

Всички авторски и сродни права върху произведения, обект на закрила на Закона за авторското право и сродните му права, включително, но не само, компютърните програми, техният изходен програмен код, структурата и дизайнът на интерфейсите и базите данни, чието разработване е включено в предмета на поръчката, възникват за Възложителя в пълен обем без ограничения в използването, изменението и разпространението им и представляват произведения, създадени по поръчка на Възложителя съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права;

Приложимите и допустими лицензи за софтуер с отворен код са:

* GPL (General Public License) 3.0
* LGPL (Lesser General Public License)
* AGPL (Affero General Public License)
* Apache License 2.0
* New BSD license
* MIT License
* Mozilla Public License 2.0

Всички доработки и/или новосъздадени софтуерни модули в рамките на настоящата поръчка, стават собственост на възложителя след окончателното им приемане.

Изпълнителят е длъжен да предаде пълния комплект програмни (сорс) кодове на разработените или модифицирани от него компоненти на единната информационно-комуникационна среда, придружени със съответната техническа документация.

Изпълнителят гарантира, че услугите, във вида на тяхното предоставяне, не накърняват права на интелектуалната собственост на трети страни.

Системата трябва да включва и доставка и инсталиране на необходимите за нейното нормално функциониране лицензи и поддръжка, като Изпълнителят трябва да предвиди и всички разходи за лицензи за външни приложения, софтуери или други програми, ако са необходими за пълноценната работа на Системата;

Всички лицензи трябва да бъдат включени в общата цена на Договора.

Изходният код (Source Code), разработван по проекта, както и цялата техническа документация не може да бъдат публично достъпни онлайн като софтуер с отворен код от първия ден на разработка чрез използване на система за контрол на версиите и хранилището по чл. 7в, т.18 от ЗЕУ, на основание Приложение 1 към чл. 25 от ЗЗКИ.

На основание Приложение 1 към чл. 25 от ЗЗКИ не може да бъде предвидено използването на Система за контрол на версиите и цялата информация за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, да бъде достъпна публично, онлайн, в реално време.

### Системна и приложна архитектура

Надграждането на Портала за МИС, наричан по-долу Система, трябва да бъде реализирано със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки. Съществуващите модули функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящето изискване.

Бизнес процесите и услугите трябва да бъдат проектирани колкото се може по-независимо с цел по-лесно надграждане, разширяване и обслужване. Системата трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс.

При разработката, тестването и внедряването на Системата, Изпълнителят трябва да прилага наложили се архитектурни (SOA, MVC или еквивалентни) модели и дизайн-шаблони, както и принципите на обектно ориентирания подход за разработка на софтуерни приложения;

Системата трябва да бъде реализирана със софтуерна архитектура, ориентирана към услуги - Service Oriented Architecture (SOA).

Взаимодействията между отделните модули в Системата и интеграциите с външни информационни системи трябва да се реализират и опишат под формата на уеб-услуги (Web Services). За всеки от отделните модули/функционалности на Системата следва да се реализират и опишат приложни програмни интерфейси.

Application Programming Interfaces (API). Приложните програмни интерфейси трябва да са достъпни и за интеграция на нови модули и други вътрешни или външни системи.

Приложните програмни интерфейси и информационните обекти задължително да поддържат атрибут за версия;

Версията на програмните интерфейси, представени чрез уеб-услуги, трябва да поддържа версията по един или няколко от следните начини:

* + - * Като част от URL-а
			* Като GET параметър
			* Като HTTP header (Accept или друг)

За всеки отделен приложен програмен интерфейс трябва да бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи (.NET, Java, PHP).

Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля;

При разработването на Системата трябва да се предвидят възможни промени, продиктувани от непрекъснато променящата се нормативна, бизнес и технологична среда. Основно изискване се явява необходимостта информационната система да бъде разработена като гъвкава и лесно адаптивна, като отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси;

Изпълнителят трябва да осигури механизми за реализиране на бъдещи промени в Системата без промяна на съществуващия програмен код. Когато това не е възможно, времето за промяна, компилиране и пускане в експлоатация трябва да е сведено до минимум. Бъдещото развитие на Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, промени във външни системи, интегрирани със Системата, отстраняване на констатирани проблеми, промени в модела на обслужване и др. Такива промени ще се извършват през целия период на експлоатация на Системата, включително и по време на гаранционния период.

Архитектурата на Системата и всички софтуерни компоненти (системни и приложни) трябва да бъдат така подбрани и/или разработени, че да осигуряват работоспособност и отказоустойчивост на Системата, както и недискриминационно инсталиране (без различни условия за инсталиране върху физическа и виртуална среда) и опериране в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак (ДХЧО).

Изпълнителят трябва да проектира, подготви, инсталира и конфигурира като минимум следните среди за Системата: тестова, стейджинг, продуктивна.

Системата трябва да бъде разгърната върху съответните среди (тестова за вътрешни нужди, тестова за външни нужди, стейджинг и продуктивна).

Тестовата среда за външни нужди трябва да бъде създадена и поддържана като "Sandbox", така че да е достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или бизнеса, с цел по-лесно и устойчиво интегриране на съществуващи и бъдещи информационни системи. Тестовата среда за външни нужди трябва да е напълно отделна от останалите среди и нейното използване не трябва да влияе по никакъв начин на нормалната работа на останалите среди или да създава каквито и да било рискове за информационната сигурност и защитата на личните данни.

Мрежата на държавната администрация (ЕЕСМ) ще бъде използвана като основна комуникационна среда и като основен доставчик на защитен Интернет капацитет (Clean Pipe) – изискванията на софтуерните компоненти по отношение на използвани комуникационни протоколи, TCP портове и пр. трябва да бъдат детайлно документирани от Изпълнителя, за да се осигури максимална защита от хакерски атаки и външни прониквания чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и ЕЕСМ.

В Техническото си предложение участникът трябва да опише добрите практики, които ще прилага по отношение на всеки аспект от системната и приложната архитектура на Системата.

За търсене трябва да се използват системи за пълнотекстово търсене (например Solr, Elastic Search). Не се допуска използването на индекси за пълнотекстово търсене в СУБД.

Всеки обект в системата трябва да има уникален идентификатор.

Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис.

Изисквания към хардуера:

- Доставката на сървъри и всякакъв друг хардуер е извън обхвата на настоящата поръчка. Всички надградени или новоразработени програмни модули трябва да могат да работят на виртуални машини всяка с до 4 процесорни ядра и минимум 8 GB RAM, със сървърни операционни системи Windows Server 2012, в рамките на съществуващата виртуализационна среда на ведомството.

- Допълнителните функционалности трябва да бъдат реализирани чрез надграждане и разширяване на съществуващата система. Извън посочените в настоящото техническо задание промени за доразвиване на портала за мрежова и информационна сигурност, Изпълнителят може да прави други съгласувани с Възложителя промени, да преработва текущата функционалност със знанието и одобрението на Възложителя или да я реализира на друга платформа, или с друга технология.

### Повторно използване (преизползване) на ресурси и готови разработки

Надграждането на Портала за МИС следва максимално да преизползва налични публично достъпни инструменти, библиотеки и платформи с отворен код.

При установяване на наличие на нови версии на използваните проекти се извършва анализ на влиянието върху настоящата система. В случаите, при които се оптимизира използвана функционалност, отстраняват се пропуски в сигурността, стабилността или бързодействието, новата версия се извлича и използва след успешното изпълнение на интеграционните тестове.

### Изграждане и поддръжка на множество среди

Изпълнителят трябва да изгради и да поддържа минимум следните логически разделени среди на собствена инфраструктура:

|  |  |
| --- | --- |
| Среда | Описание |
| Development | чрез Development средата се осигурява работата по разработката, усъвършенстването и развитието на Системата. В тази среда са налични и допълнителните софтуерни системи и инсталации, необходими за управление на разработката – continuous integration средства, системи за автоматизирано тестване и др. |
| Staging | чрез Staging средата се извършват тестове преди разгръщане на нова версия от Development средата върху Production средата. В нея се извършват всички интеграционни тестове, както и тестовете за натоварване. |
| Production | това е средата, която е публично достъпна за реална експлоатация и интеграция със съответните външни системи и услуги. |

### Процес на разработка, тестване и разгръщане

В случай че върху част от компонентите, нужни за компилация, има авторски права, те могат да бъдат или в отделно хранилище с подходящия за това лиценз или за тях трябва да бъде предоставен заместващ „mock up“ компонент, така че да не се нарушава компилацията на проекта.

Трябва да се анализират възможностите за включване на граждани в процесите по разработка, тестване и идентифициране на пропуски на софтуера. Участникът трябва да предложи механизъм и процедури за реализирането на такива процеси.

За всеки един разработван компонент Изпълнителят трябва да покрие следните изисквания за гарантиране на качеството на извършваната разработка и на крайния продукт:

• Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас;

• Покритие на минимум 50% от изходния код с функционални тестове [в случай на надграждане на съществуваща система – 50% от новата функционалност и 20% от съществуващата];

• Използване на continuous integration практики;

• Използване на dependency management.

Участникът трябва да опише детайлно подхода си за покриване на изискванията.

Във всеки един компонент на Системата, който се build-ва и подготвя за инсталация (deployment), е необходимо да присъстват следните реквизити:

• Дата и час на build;

• Място/среда на build;

• Потребител извършил/стартирал build процеса;

• Идентификатор на ревизията от кодовото хранилище на компонента, срещу която се извършва build-ът.

### Подписване на документи

В съществуващата система се поддържа подписване на електронни изявления и електронни документи с електронни подписи, издадени от Доставчици на доверителни услуги в ЕС, които отговарят на изискванията за унифициран профил на електронните подписи, съгласно подзаконовите правила към Регламент ЕС 910/2014.

### Бързодействие и мащабируемост

#### Контрол на натоварването и защита от DoS/DDoS атаки

Системата трябва да поддържа на приложно ниво "Rate Limiting" и/или "Throttling" на заявки от един и същ клиентски адрес, както към страниците с уеб-съдържание, така и по отношение на заявките към приложните програмни интерфейси, достъпни публично или служебно като уеб-услуги (Web Services) и служебни интерфейси.

Системата трябва да позволява конфигуриране от страна на администраторите на лимитите за отделни страници, уеб-услуги и ресурси, които се достъпват с отделен URL/URI.

Системата трябва да поддържа възможност за конфигуриране на различни лимити за конкретни автентикирани потребители (напр. системи на други администрации) и трябва да предоставя възможност за генериране на справки и статистики за броя заявки по ресурси и услуги.

#### Бързодействие

В Етап 1: Анализ и проектиране Изпълнителя трябва да проведе необходимите тестове за натоварване на система, да анализира получените резултати и да направи съответните препоръки за подобряване на бързодействието. След реализиране на новите функционални изисквания, преди окончателното внедряване на системата, процедурата трябва да се повтори и да се гарантира минимално време за отговор на заявки, като средното време за заявка трябва да бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките.

Трябва да бъдат създадени тестове за натоварване. За проведените тестове с участието на CERT BG, да бъдат подписани констативни протоколи.

#### Използване на HTTP/2

С оглед намаляване на служебния трафик, времената за отговор и натоварването на сървърите следва да се използва HTTP/2 протокол при предоставяне на публични потребителски интерфейси с включени като минимум следните възможности:

* Включена header compression;
* Използване на brotli алгоритъм за компресия;
* Включен HTTP pipelining;
* HTTP/2 Server push, приоритизиращ специфични компоненти, изграждащи страниците (CSS, JavaScript файлове и др.);
* Публичните потребителски интерфейси трябва да поддържат адаптивен избор на TLS cipher suites според вида на процесорната архитектура на клиентското устройство - AES-GCM за x86 работни станции и преносими компютри (с налични AES-NI CPU разширения), и ChaCha20/Poly1305 за мобилни устройства (основно базирани на ARM процесори);
* Ако клиентският браузър/клиент не поддържа HTTP/2, трябва да бъде предвиден fall-back механизъм към HTTP/1.1. Тази възможност трябва да може лесно да се реконфигурира в бъдеще и да отпадне, когато браузърите/клиентите, неподдържащи HTTP/2, станат незначителен процент.

#### Качество и сигурност на програмните продукти и приложенията

Да бъде предвидено спазването на добри практики на софтуерната разработка – покритие на изходния код с тестове – над 60%, документиране на изходния код, използване на среда за непрекъсната интеграция (Continuous Integration), възможност за компилиране и пакетиране на продукта с една команда, възможност за инсталиране на нова версия на сървъра с една команда, система за управление на зависимостите (Dependency Management);

Публичните модули, които ще предоставят информация в Интернет, трябва да отговарят на актуалните уебстандарти за визуализиране на съдържание.

### Информационна сигурност и интегритет на данните

Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption);

Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата;

Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Internet Explorer, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката;

Трябва да бъдат извършени тестове за сигурност на всички уебстраници, като минимум чрез автоматизираните средства на SSL Labs за изпитване на сървърна сигурност (https://www.ssllabs.com/ssltest/).

Като временна мярка за съвместимост настройките на уебсървърите и Reverse Proxy сървърите трябва да бъдат балансирани така, че приложенията да позволяват използване и на клиентски браузъри, поддържащи по-стария протокол TLS 1.1. Това изключение от общите изисквания за информационна сигурност не се прилага за достъпа на служебни потребители от държавната администрация,услуги, които имат служебен достъп до ресурси на приложенията;

При разгръщането на всички уеб услуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2;

Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за оперативна съвместимост и информационна сигурност;

При проектирането и разработката на уеб приложенията и интерфейсите и при подготовката и разгръщането на средите трябва да се спазват последните актуални препоръки на OWASP (Open Web Application Security Project);

Трябва да бъде изграден модул за проследимост на действия и събития в надградената АИС за инвентаризация на ИКИ ресурсите . За всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:

* + - * Уникален номер;
			* Точно време на възникване на събитието;
			* Вид (номенклатура от идентификатори за вид събитие);
			* Данни за информационна система, където е възникнало събитието;
			* Име или идентификатор на компонент в информационната система, регистрирал събитието;
			* Приоритет;
			* Описание на събитието;
			* Данни за събитието.

Астрономическото време за удостоверяване настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при технологична необходимост - милисекунда, изписани в съответствие със стандарта БДС ISO 8601:2006;

Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставимост, трябва да бъде удостоверявано с електронен времеви печат по смисъла на Глава III, Раздел 6 от Регламент ЕС 910/2014. Трябва да бъде реализирана функционалност за получаване на точно астрономическо време, отговарящо на горните условия, и от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161;

Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността.

 Изпълнителят трябва да предприеме всички необходими мерки, за да осигури пълното съответствие на системата със специфичните законови и подзаконови изисквания по отношение на оперативна съвместимост и информационна сигурност. Към момента те произтичат основно от Закона за електронното управление (ЗЕУ), Наредбата за общите изисквания за мрежова и информационна сигурност (НОИМИС) и други свързани с тях подзаконови нормативни актове. Изпълнителят следва да се съобрази с текущото състояние на законодателството в актуалния му вид към момента на изпълнението на проекта.

### Използваемост

Наред със специфичните изисквания по отношение на функционален и информационен обхват, всички надградени или новоразработени софтуерни модули и компоненти трябва да отговарят на определени общи изисквания към потребителския интерфейс, като:

* + Потребителският интерфейс да е на български език и да поддържа утвърдените стандарт за кирилица UTF8.
	+ Потребителският интерфейс трябва да е лесен за използване, интуитивен и лесен за възприемане.
	+ Потребителският интерфейс трябва да е хомогенен и еднотипен, със стандартизирани контроли и визуални елементи, с цел бързо усвояване и лесно използване.
	+ Потребителският интерфейс трябва да е WEB-базиран, да работи на повечето популярни интернет-браузъри и да не изисква инсталиране на софтуер на потребителските работни места (освен изрично упоменати изключения, предназначени за силно ограничен брой специализирани работни места).
	+ Визията на потребителския интерфейс трябва да е съобразена с общата визия на Портала за мрежова и информационна сигурност govcert.bg. В случаите когато се налага промяна, то тя да се извърши след предварително одобрение от страна на Възложителя след представяне на проекто-дизайн.

Публичната част на Системата трябва да позволява превключване между работните езици на потребителския интерфейс в реално време от профила на потребителя и от подходящ, видим и лесно достъпен навигационен елемент, който включва не само текст, но и подходяща интернационална икона за съответния език;

При визуализация на дати и точно време в елементи от потребителския интерфейс в генерирани справки или в електронни документи всички формати за дата и час трябва да са съобразени с избрания от потребителя език/локация в настройките на неговия профил:

* За България стандартният формат е „DD.MM.YYYY HH:MM:SS”, като наличието на време към датата е в зависимост от вида на визуализираната информация и бизнес-смисъла от показването на точно време;
* Системата трябва да поддържа и всички формати, съгласно
ISO БДС 8601:2006;

Всички ресурси трябва да са достъпни чрез GET заявка на уникален адрес (URL). Не се допуска използване на POST за достигане до формуляр за подаване не заявление, за генериране на справка и други.

Не се допуска използване на капча (Captcha) като механизъм за ограничаване на достъпа до документи и/или услуги. Допуска се използването на Captcha единствено при идентифицирани много последователни опити от предполагаем „бот“.

Публичните уеб страници на Системата трябва да бъдат проектирани и оптимизирани за ефективно и бързо индексиране от търсещи машини с цел популяризиране сред потребителите и по-добра откриваемост при търсене по ключови думи и фрази. При разработката на страниците и при изготвяне на автоматизираните процедури за разгръщане на нова версия на Системата трябва да се използват инструменти за минимизиране и оптимизация на размера на изходния код (HTML, JavaScript и пр.) с оглед намаляване обема на файловете и по-бързо зареждане на страниците.

При разработката на публични уеббазирани страници трябва да се използват и да се реализира поддръжка на:

* Стандартните семантични елементи на HTML5 ([HTML Semantic Elements](http://www.w3schools.com/html/html5_semantic_elements.asp));
* JSON-LD 1.0 (<http://www.w3.org/TR/json-ld/>);
* Open Graph Protocol (<http://ogp.me>) за осигуряване на поддръжка за качествено споделяне на ресурси в социални мрежи и мобилни приложения;
* Не се допуска използването на Flash-базирано съдържание.

Всяка екранна форма трябва да има наименование, което да се изписва в горната част на екранната форма. Наименованията трябва да подсказват на потребителя какво е предназначението на формата.

Всички търсения трябва да са нечувствителни към малки и главни букви.

Полетата за пароли трябва задължително да различават малки и главни букви.

Главните и малките букви на въвежданите данни се запазват непроменени, не се допуска Системата да променя капитализацията на данните, въвеждани от потребителите.

Наименованията на полетата следва да са достатъчно описателни, като максимално се доближават до характера на съдържащите се в тях данни.

Системата трябва да поддържа прекъсване на потребителски сесии при липса на активност. Времето трябва да може да се променя от администратора на системата без промяна в изходния код. Настройките за време за прекъсване на неактивни сесии трябва да включват и възможността администраторите да дефинират стилизирана страница с информативно съобщение, към която Системата да пренасочва автоматично браузърите на потребителите в случай на прекъсната сесия.

Дългите списъци с резултати трябва да се разделят на номерирани страници с подходящи навигационни елементи за преминаване към предишна, следваща, първа и последна страница, към конкретна страница. Навигационните елементи трябва да са логически обособени и свързани със съответния списък и да се визуализират в началото и в края на контейнера, съдържащ списъка.

По време на въвеждане на текст в полета за търсене и задаване на номенклатура, да се появява списък със съвпадения от списъка с номенклатури.

### Системен журнал

Изгражданото решение за Уеб приложението реализиращо регистъра на информационните ресурси задължително трябва да осигурява проследимост на действията на всеки потребител (одит), както и версия на предишното състояние на данните, които той е променил в резултат на своите действия (системен журнал).

 Атрибутите, които трябва да се запазват при всеки запис, трябва да включват като минимум следните данни:

* дата/час на действието;
* модул на системата, в който се извършва действието;
* действие;
* обект, над който е извършено действието;
* допълнителна информация;
* IP адрес и браузър на потребителя.

Размерът на журнала на потребителските действия нараства по време на работа на всяка система, което налага по-различното му третиране от гледна точка на организация на базата данни:

* по време на работа на приложението потребителският журнал трябва да се записва в специализиран компонент, който поддържа много бързо добавяне на записи; този подход се налага, за да не се забавя излишно работата на Приложението;
* специална фонова задача трябва да акумулира записаните данни и да ги организира в отделна специално предвидена за целта база данни, отделна от работната база данни на Приложението;
* данните в специализираната база данни трябва да се архивират и изчистват, като в специализираната база данни трябва да бъде достъпна информация за не повече от 2 месеца назад; при необходимост от информация за предишен период администраторът на Приложението трябва първо да възстанови архивните данни

# ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

## Функционален обхват на софтуерните разработки

Функционалният обхват на поръчката произтича от поставените цели и се разпростира върху значителен брой съществуващи системи в агенцията. Обхватът може условно да се раздели на няколко части, като всяка от тях може да обхваща разработка на нова функционалност, модификация на съществуваща функционалност, редизайн и/или оптимизация на потребителски интерфейс (отделни форми и елементи в една, повече или всички страници), драстични промени или интеграция с една или повече от системите във ведомството.

## Разширяване на функционалния обхват на портала за мрежова и информационна сигурност

Към настоящия момент, след над 4-годишно функциониране, в портала за мрежова и информационна сигурност на Агенцията има регистрирани над 3452 инцидента в мрежовата и информационната сигурност. Наблюдението на използваемостта на отделните функционалности на портала, заедно със събраната обратна връзка от неговите ползватели, представляват една достатъчно добра основа за формулирането на зони за подобряване.

Въз основа на това е идентифицирана необходимост от следните функционални подобрения на портала:

## Разработване на модул за обработване на постъпващи външни заявки и доклади

За оказване реактивна помощ на административните органи при иницииране на събитие, заявка и инцидент в информационната сигурност и обработка на сигнали за нарушения в и от Българското Интернет пространство в дирекцията се прилага разработен и утвърден алгоритъм на работа - *Приложение - Процедура за обработка на инциденти.*

Процеса на обработка на сигналите за нарушение от и във българското интернет пространство започва с получаване на самия сигнал. Съществуват няколко комуникационни канала, по които сигналите за инциденти постъпват в **CERTbg**:

а) За регистрираните служители за мрежова и информационна сигурност на конституентите - чрез попълване на формата на портала за МИС (мрежова и информационна сигурност) на адрес www.govcert.bg;

б) Чрез попълване на WEB формата на портала за МИС: на адрес [www.govcert.bg](http://www.govcert.bg);

в) Чрез Електронна административна услуга: през портала на адрес [www.govcert.bg](http://www.govcert.bg);

г) по електронната поща на адрес: cert@govcert.bg и govcert@govcert.bg;

д) на телефон: +359 2 949 2212; GSM +359 878 908 546;

е) по факс: +359 2 949 2211;

Най-голям е делът на постъпващите сигнали чрез електронната поща. Въвеждането им в портала на този етап е ръчно и съществува голяма вероятност от допускане грешки и забавяне на процеса. Освен това се налага веднъж да се отговори на докладващия, какво се случва с неговия сигнал и да се уведомят засегнатите ISP или конституенти през електронната поща и втори път след това тези действия да се въвеждат ръчно в портала. Това е причината да се пристъпи към разработване на модул за автоматично обработване на постъпващи външни заявки и доклади, интегриран с вътрешните модули на системата.

Модулът ще подпомогне обслужването на пристигащите по е-mail заявки чрез въвеждане на автоматизиран подход за създаване на инцидент (е-mail към инцидент).

Автоматизирането на процеса (Внедряването на модула) трябва да се направи така, че в мейл сървъра да остава следа за всички получени и изпратени мейли през портала. Агенцията използва Microsoft Exchange server 2016.

Функционирането на тикет системата (модула за обработка на външни заявки) трябва напълно да отговаря на утвърдената процедура за обработка на инциденти в Дирекция МИС (виж Приложение 1).

## Добавяне на нови функционалности и доработка на съществуващи в модул „Инциденти“

### Разработване на типови шаблони за инциденти в модул „Инциденти“

Да се разработи нова функционалност „шаблон за типови инциденти“, чрез който автоматично се попълват данни в съответствие с разработения шаблон за съответния типов инцидент.

Тази функционалност дава възможност:

* както за автоматично допълване на всички непопълнени от тикет системата полета, намалявайки значително времето за ръчна обработка.
* така и при нов отворен инцидент да се попълнят всички зададени полета според шаблона.

С тази функционалност ще се спести много време за ръчно въвеждане на детайли от инцидента.

### Автоматична обработка едновременно на множество IP адреси на засегнати системи

В модул „Инциденти“ се проследява целия цикъл на обработка на сигнала от регистрирането му като инцидент до неговото разрешаване. Процесът преминава през класифициране на инцидента; определяне на засегнатите страни; проверка за стари инциденти, свързани с този IP адрес; изпращане на писма на засегнатите страни; въвеждане на получените отговори; изпращане на допълнителна информация; въвеждане на информация от евентуално проведен телефонен разговор – входящ или изходящ и затваряне на инцидента. Всички гореспоменати действия са ръчни и това налага най-много промени да бъдат направени в този модул с цел максимално автоматизиране на работата.

Към модул „Инциденти“ трябва да се добави нова функционалност за автоматична обработка на IP адреси на засегнати системи:

1. Импорт на списък с IP адреси на засегнати системи от файл със структурирана информация при обработка на инциденти.
2. Автоматична проверка за обхвата на въведените IP адреси на засегнатите системи – в адресите на конституентите на CERT България и на интернет доставчиците чрез съпоставяне на данните, налични в портала и тези, фигуриращи в база данните за ISP-тата в RIPE.
3. Автоматично въвеждане на данните на засегнатите страни, установени от проверката по т.2 – наименование на засегната страна, засегнати IP адреси, e-mail и др. полезна информация.
4. Възможност за изпращане на автоматични уведомления по електронна поща до участниците по предварително зададен шаблон с обобщени данни за всички IP адреси участващи в конкретния инцидент от неговата мрежа.
5. Възможност за едновременно прикачване на множество файлове при изпращане на уведомление.
6. Регистриране на всички изпратени в хронологията на инцидента.
7. Изпратените уведомления трябва да оставят копие/следа в мейл сървъра на ДА ЕУ.
8. Промяна на формата на въвеждане на данните в поле „IP адрес“.
9. Трябва да се разшири функцията за търсене по IP адрес посредством обединяване на резултати от различни масиви с информация.
10. Разработване на функционалност за проверка и подходяща обработка (създаване на нов инцидент или добавяне на последващ доклад към регистриран такъв) въз основа на повторяемостта на постъпилите сигнали за докладваните IP адреси.

В техническото си предложение кандидатите трябва да представят подход за реализация на автоматичната обработка на IP адреси на засегнати системи.

### Модифициране на „Хронология“

В модул „Инциденти“, в раздел „Хронология“ се отбелязват всички извършени операции от отговорника, обработващ инцидента, както и да се записват действията по разрешаването му. Необходимо е да се разграничат действията по обработка на инцидента от хронологичните операции в системата, като по този начин се гарантира логичната последователност на процесите и хронологична подредба на регистрираните събития.

### Модифициране на информацията в някои от екраните / отделните менюта

* Извеждане на информация за засегнатите IP адреси в меню „Инциденти“
* Извеждане на данни за засегнатата страна в модул „Инциденти“
* Извеждане на информация за засегнати IP адреси в модул „Инциденти“
* Възможност за избор на участници (един, повече, всички) при изпращане на автоматични уведомления в модул „Инциденти“, секция „Участници“.
* Въвеждане на промени по отношение на извеждане на данни за е-mail адрес на участниците в модул „Инциденти“, секция „Участници“
* Указване на IP адреса (един или повече), засегнат от свързания инцидент - модул „Инциденти“, секция „Свързани инциденти“

### Оптимизация на форми, редизайн

С оглед оптимизиране на работата по обработка на инцидента в портала, в модул „Инциденти“ е необходимо да се промени статута на някои от задължителните полета за попълване. При реалното използване на системата се оказа, че има полета, които не е необходимо да бъдат задължително попълнени.

* Да се предвиди възможност за автоматично попълване на данни (в една или повече форми) в случай на констатирана необходимост в процеса на бизнес анализ, като се вземат предвид и изискванията, залегнали в т. 7.4.1.
* Въвеждане на промени по отношение на подредбата на елементите в модални прозорци (един или повече) с цел оптимизация на „полезното“ пространство, извеждане на допълнителни бутони за основни действия – запис, отказ.
* Необходимост от преструктуриране на секция „Хронология“ в модул „Инциденти“ с оглед интегриране на тикет системата. Виж подробности в т. 7.3.
* Оптимизация на други форми, включително редизайн по искане на Възложителят и при констатирана необходимост в етап Бизнес анализ и проектиране.

## Преструктуриране на интерфейса за наливане на уязвимости в портала, модул „Уязвимости“

В модул „Уязвимости“ на портала за МИС автоматично се наливат уязвимостите, ползвайки като източник National Vulnerability Database (NVD) на САЩ. В този модул се осъществява и връзката между уязвимостите и базата данни със софтуера и хардуера, използван от конституентите, което позволява на потребителите да виждат, както всички налични уязвимости, така и само тези, които се отнасят конкретно за тяхната инсталационна база. При промяна структурата на информацията подавана от NVD се налага корекция на схемата на съпоставяне с полетата от базата в портала, затова е необходимо системата да е гъвкава и адаптивна при промени на входните данни. За целта трябва да се разработят процедури за:

* събиране на информацията за уязвимостите в базата;
* съпоставянето на уязвимостта с инсталационната база данни на конституентите.

Трябва да бъде обучен екипът на CERT BG да прилага съответните процедури.

Осъществяване на връзката с мейл сървъра, с оглед извършване предоставяне на ЕАУ и автоматично известяване по е-mail (до отговорниците по МИС) през системата за новорегистрирани уязвимости (Винаги трябва да остава следа в пощенската кутия за изпратените писма).

В техническото си предложение кандидатите трябва да представят подробно разписана процедура по наливане на уязвимости

### Адаптиране към обновената структура на данните в CVE списъците (Common Vulnerabilities and Exposures List)

В рамките на обхвата на проекта, Изпълнителят следва да извърши необходимите корекции в схемата на съответствие между полетата от базата в портала и данните, съдържащи се в актуализираните CVE списъци, като по този начин осигури възможност за периодично обновяване на CVE списъка.

В техническото си предложение кандидатите трябва да представят подробно разписана процедура за актуализация на CVE списъците

## Доразвиване на функционалността за изпращане на информационни бюлетини

Изпращането на информационни бюлетини за новооткрити уязвимости е една от четирите ЕАУ, които CERT България предоставя на своите конституенти. В сегашната си реализация се изпраща е-мейл с информация за новоизлезлите уязвимости, отговарящи на използвания софтуер и хардуер от конституентите, само ако се е абонирал. Да се предвиди активиране по подразбиране за всички регистрирани конституенти, а ЕАУ да е за отказ от абонамент. На потребител с роля Администратор на системата да се даде право на редакция на тази функционалност.

## Доразвиване на функционалността „Сортиране по колони“

Това е една от възможностите за бърза справка и търсене в системата, която е реализирана частично само в меню „Инциденти“. Тази възможност следва да се приложи и по отношение на останалите модули на Портала.

Необходимо е да бъде доразвита функционалността за сортиране на всички колони в модулите „Уязвимост“, „Инциденти“, „Конституенти“, „Участници“, „Интернет доставчици“, „Партньори“, „Администриране“.

## Оптимизиране на формата за докладване на инциденти

Съществуват няколко начина за докладване на инциденти:

* чрез е-мейл
* чрез ЕАУ
* чрез WEB формата за докладване на инциденти през уеб сайта за нерегистрирани потребители
* като регистриран потребител през портала.

Формата за докладване на инциденти е достъпна през уеб сайта [www.govcert.bg](http://www.govcert.bg) за нерегистрирани потребители.

След изпращане на успешно попълнена форма за докладване, въведената от потребителя информация следва автоматично да се попълва в системата. За реализиране на тази функционалност е необходимо да се преработят полетата във формата, до гарантиране на пълно съответствие с полетата в системата.

Необходимо е да се надгради функционалността чрез:

* извеждане на уведомително съобщение за потвърждение на успешно реализирана операция или указване на причините за грешка, в случай че е констатирана такава;
* в пощенската кутия cert@govcert.bg да се получи известие за постъпил сигнал в портала.

## Осигуряване на връзка с изграждащия се Регистър на информационни активи

Осъществявайки основната идея на електронното управление, а именно веднъж въведени данни да се използват многократно е необходимо да се осъществи връзка между портала за МИС и проекта за инвентаризация на информационните активи в държавната администрация. Тази интеграция на данните ще даде възможност на нашите конституенти да получават актуална информация за уязвимостите в техните информационни активи, защото първоначалната информация в базата е събирана през 2013 г.

Да се реализира автоматизиран онлайн обмен на данни между изграждащия се Регистър на информационни активи и Портала за мрежова и информационна сигурност на Република България, чрез идентификация на информационните активите съгласно National Institute of Standards and Technology (NIST) - Common Platform Enumeration (СРЕ) (https://scap.nist.gov/specifications/cpe/), за обобщени данни подробно уточнени в етапа на анализ, описани в софтуерна спецификация.

Минималните обобщени данни за конкретна административна структура (Наименование, Тип, Подтип, ЕИК) са описани по-долу:

1. Обобщени данни за обща софтуерна инсталационна база – операционни системи и приложни софтуери по вид:
	* Статус на софтуера;
	* Тип/Вид на софтуера.
2. Обобщени данни за мрежово оборудване:
	* Статус на хардуера;
	* Тип/Вид на мрежовото оборудване;
	* Тип IP address;
	* IP address.
3. Обобщени данни за сървърно оборудване:
	* Статус на сървърното оборудване;
	* Тип/Вид на софтуера;
	* Роля на сървъра;
	* Тип/вид на машината (или виртуална);
	* Тип IP address;
	* IP address.
4. Обобщени данни за публични мрежови адреси:
	* Данни за начален и краен IP адрес от обхвата;
	* Указване на повече от един обхват от IP адреси.

Изпълнителят на настоящия проект следва да подготви необходимия вход към портала, съответстващ на залегналите в анализа изисквания за осъществяване на обмен на данни между двете системи.

**Периодичност на обновяване на данните**

В процеса на анализ и проектиране на техническото задание за „Инвентаризация на информационно-комуникационната инфраструктура за нуждите на електронното управление“ следва да бъде уточнена динамиката на извършваните промени и нуждата от периодична актуализация, както и интервалите на нейното обновяване.

## Подобряване на бързодействието на системата

В Етап 1: Анализ и проектиране Изпълнителя трябва да проведе необходимите тестове за натоварване на система, да анализира получените резултати и да направи съответните препоръки за подобряване на бързодействието. След реализиране на новите функционални изисквания, преди окончателното внедряване на системата, процедурата трябва да се повтори и да се гарантира минимално време за отговор на заявки, като средното време за заявка трябва да бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките.

За тестовете, проведени с участието на CERT BG, да бъдат подписани констативни протоколи.

## Справочна система - Разработка на генератор на справки и отчети

Изпълнителят на настоящия проект трябва да внедри, работещо решение за генериране на справки и отчети. Справочният модул трябва да предостави интерфейс на потребителите за задаване на критерии и представяне на резултатите от изпълнението на конкретни справки. Справочната система трябва разполага със следната функционалност:

* Задаване на филтри по различни критерии преди извличане на резултатите;
* Задаване на начин на сортиране на резултатите;
* Представяне на резултатите от справка в табличен вид;
* Представяне на резултатите от справка във вид на диаграма;
* Комбинирани справки, включващи резултати в табличен вид и диаграми;
* Да се указват колоните, които да бъдат включени в справката и техните параметри;
* Възможност за отпечатване по предварително дефинирани образци;
* Справките трябва да могат да се експортират във файлове в стандартен формат (минимум xls); Справките трябва да могат да се визуализират по прегледен начин на екран, а също така да се съхраняват локално на компютър, минимум в следните формати:
* Структурирана Excel – таблица за справките, чиито резултат представлява табличен списък с резултати за повече от един обект на индустриалната собственост;
* PDF – документ
* Възможност за създаване на логическа връзка между различни таблици и изгледи;
* Възможност за съхраняване на предефинирани справки - филтри, колони, сортиране, образец, вид диаграма и др. параметри.

При реализацията на справочната система Изпълнителят трябва да създаде в базата данни представящ слой на данните, предназначен за генериране на справки. Трябва да бъдат изготвени изгледи за следните информационни области на системата:

* Уязвимости;
* Инциденти;
* Конституенти;
* Участници;
* Партньори;
* Интернет доставчици.

Справочният модул трябва да включва като минимум следните работни места:

* Създаване и редакция на шаблони за отчети – минимум две работни места;
* Изпълнение и преглед на отчети – минимум пет работни места.

В случай, че предлаганото решение изисква използването на базов софтуер, то кандидатът трябва да достави необходимите лицензи.

Така създадените справки трябва да бъдат добре документирани и служителите на отдела, трябва да бъдат обучени как да променят тяхната дефиниция при необходимост, и/или да създават нови справки.

В техническото си предложение кандидатите трябва да представят подход за реализация на справочната система.

## Обновяване дизайна на публичната част на портала за МИС [www.govcert.bg](http://www.govcert.bg)

Визията на сайта не е променена от неговото създаване през 2009 г. Бързопроменящите се тенденции в разработване на подобни сайтове, довежда до необходимостта за актуализиране и промяна дизайна на уеб сайта.

В публичната част на портала да има възможност за търсене по израз, дума и/или дата на публикуване в разделите „Предупреждения“, „Съвети“, „Новини“.

Ограничението в обема и формата на материалите, които са в публичната част на портала в разделите „Предупреждения“, „Съвети“, „Новини“ да може да бъде контролирано.

Да има гъвкавост при избор на език, на който ще се публикуват материалите в разделите „Предупреждения“, „Съвети“, „Новини“ и адекватна визуализация.

В техническото си предложение кандидатите трябва да представят подходящ дизайн на уеб сайта, който трябва да бъде лесен за използване, интуитивен и лесен за възприемане

## Разработване на експлоатационна документация

В процеса на експлоатация на портала понякога се налага да бъде рестартирана системата, да бъде инсталиран нов SSL сертификат, да бъде възстановена от архив базата или др. С оглед на реализираните промени във функционалността на портала е необходимо Изпълнителят да изготви и предаде следните кратки инструкции и процедури:

* Инструкция за инсталиране на SSL сертификат;
* Процедура за наливане на уязвимости;
* Обновяване на CPE версията, която се ползва при въвеждане на инсталационната база данни на конституентите;
* Процедура за съпоставяне на инсталационната база данни с уязвимостите;
* Инструкция за RSS – на вируси и уязвимости, реализирана на уеб сайта;
* Процедура за спиране и пускане на вътрешния модул и уеб сайта;
* Процедура за възстановяване на системата от архив;
* Процедура за архивиране на системата;
* Инструкции за прилагане на актуализации на всеки един от софтуерните компоненти, изграждащи портала.
* Процедура за обработка на множество IP адреса

В тестовия период, преди внедряване на системата в продукционна среда, трябва да бъдат проиграни всички гореспоменати процедури от персоналът на CERT BG и за резултатите да се състави констативен протокол, подписан от двете страни.

# ДОКУМЕНТАЦИЯ

## Изисквания към документацията

Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително и на нейните съставни части, трябва да бъдат налични и на български език;

Всички документи трябва да бъдат предоставени от Изпълнителя в електронен формат (ODF/ /Office Open XML/MS Word DOC/RTF/PDF/HTML или др.), позволяващ пълнотекстово търсене/търсене по ключови думи и копиране на части от съдържанието от оригиналните документи във външни документи, за вътрешна употреба на възложителя;

Навсякъде, където в документацията има включени диаграми или графики, те трябва да бъдат вградени в документите в оригиналния си векторен формат;

Детайлна техническа документация на програмния приложен интерфейс (API), включително за поддържаните уебуслуги, команди, структури от данни и др.

Детайлна техническа документация за схемата на базата данни – структури за данни, индекси, дялове, съхранени процедури, конфигурации за репликация на данни и др.

Цялата документация по изпълнението трябва да отговаря на определени стандарти и утвърдени добри практики по отношение на оформление, структура, контрол на версиите, критерии за проследимост и контрол на качеството на документите. Изпълнителят следва да предложи стандарти за подготовка на документация, съобразени с предлаганата от него проектна методология.

## Прозрачност и отчетност

Всички документи се изготвят на български език и се предоставят в един хартиен екземпляр и на електронен носител.

## Системен проект

Изпълнителят на настоящата поръчка трябва да дефинира в детайли конкретния обхват на реализация на софтуерната разработка и да документира изискванията към софтуера в детайлна техническа спецификация (системен проект), която ще послужи за пряка изходна база за разработка.

При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва утвърдена нотация за описание на бизнес модели. Изготвената детайлна техническа спецификация (системен проект) се представя за одобрение на Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в детайлната техническа спецификация (системен проект).

## Техническа документация

При изпълнение на дейностите по настоящата поръчка, изпълнителят трябва да изготви следната техническа документация, съдържаща:

* + Ръководство за инсталиране, конфигуриране и администриране;
	+ Ръководство за потребителите;
	+ Детайлно техническо описание на софтуерните модули и базата данни;
	+ Описание на изходния програмен код

## Протоколи

Изпълнителят трябва да изготвя протоколи от изпълнението на различните етапи на проекта, описани в раздел 8 на настоящия документ, заедно със съпътстващите ги документи – резултати от изпълнението на етапите.

## Комуникация и доклади

### Встъпителен доклад

Изпълнителят следва да представи в двуседмичен срок от подписването на договора Встъпителен доклад, който включва подробен план за работата и изпълнение на дейностите по поръчката, както и описание на екипите (роли и отговорности) на изпълнителя и възложителя.

### Междинен доклад

Избраният изпълнител изготвя 1 междинен доклад в хода на изпълнение на поръчката. Докладът се представя до 5 работни дни след изготвянето на анализа и техническия проект. В доклада изпълнителят трябва да опише детайлно извършените от него действия и постигнатите резултати, възникналите проблеми и/или затруднения в хода на изпълнение на дадената дейност и мерките за тяхното преодоляване. Към доклада се прилагат копия на всички относими към изпълнението документи.

### Окончателен доклад

Изпълнителят изготвя Окончателен доклад за цялостно отчитане, приключването и предаването на извършената работа по поръчката. Проектът на окончателния доклад се представя две седмици преди срока за приключване на работата по договора. Той включва обобщена и аналитична информация и оценка за резултатите от изпълнените дейности, постигнатите цели и резултати, идентифицираните трудности и проблеми, предприетите корективни мерки и т.н.

Всички доклади се представят на хартиен и електронен носител. Те се одобряват или връщат със задължителни за изпълнителя указания за корекции от упълномощено от възложителя лице, в срок до 5 /пет/ работни дни от получаването им. Изпълнителят представя коригирания доклад в срок до 5 /пет/ работни дни от получаването на коментарите на възложителя.

Докладите се изпращат до отговорния служител на Възложителя. За тази цел Възложителят ще определи в договора отговорния/отговорните служител/служители. Всички доклади се представят на български език в електронен формат и на хартиен носител. Докладите се одобряват от отговорния/отговорните служител/служители в срок до 5 работни дни.

Всички доклади трябва да се представят на възложителя на български език на хартиен и на електронен носител. Представянето на докладите трябва да се извършва чрез подписване на двустранни предавателно-приемателни протоколи, подписани от представители на Изпълнителя и на Възложителя.

Възложителят разглежда представените доклади и уведомява Изпълнителя за приемането им без забележки или ги връща за преработване, допълване и/или окомплектоване, ако не отговарят на изискванията, като чрез упълномощено в договора лице дава указания и определя срок за отстраняване на констатираните недостатъци и пропуски.

# РЕЗУЛТАТИ

Очакваните резултати от изпълнението на настоящата обществена поръчка са следните:

* Автоматизиране на процеса на управление на инциденти;
* Нова визия на Националния портал за МИС;
* Автоматизиране на процеса на генериране на отчети, справки и статистика.