**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

# **Цел на поръчката**

Настоящата поръчка „Наблюдение и управление на ИКИ на МВнР“ има за цел да осигури доставчик на висококвалифицирани ИКТ дейности и услуги за нуждите на МВнР, чрез които да се постигнат и поддържат ниски нива на информационните рискове и да се гарантира поверителността, цялостността и наличността на трансферираната, обработваната и съхраняваната информацията в информационната и комуникационната инфраструктура (ИКИ) на МВнР.

# **Локации**

Локацията, в които следва да се изпълняват висококвалифицираните еднократни дейности и предоставят висококвалифицираните регулярни услуги е Централна сграда на МВнР – София, ул. „Ал. Жендов“ №2.

# **Обща информация**

## Продължителност на проекта

Настоящата поръчка ще формира проект с обща продължителност 24 (двадесет и четири) месеца, считано от датата на започване изпълнението по договора с Изпълнителя.

## Етапи в проекта

### Етап 1

Извършване на еднократни висококвалифицирани ИКТ дейности. Продължителност 3 (три) месеца.

### Етап 2

Предоставяне на регулярни висококвалифицирани ИКТ услуги. Продължителност 21 (двадесет и един) месеца.

### Етап 3

Защита на мрежовия трафик на МВнР чрез системи за сигурност на доставчика на висококвалифицирани ИКТ дейности и услуги.

Продължителност 24 (двадесет и четири) месеца.

### Разпределение на етапите в проекта

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Етап** | **Започване изпълнението на договора** | **Продължителност (мес.)** | | **Край на**  **проекта** |
|  | *<дата>* |  | |  |
| 1 |  | 3 |  |  |
| 2 |  |  | 21 |  |
| 3 |  | 24 | |  |
|  |  |  | | *<дата>* |

## Висококвалифицирани експерти

### Необходимо е всички висококвалифицирани ИКТ дейности и услуги за нуждите на МВнР да се извършват от експерти на Изпълнителя, притежаващи разрешение за достъп до класифицирана информация ниво „Поверително“, съгласно ЗЗКИ.

* + 1. Необходимо е всички висококвалифицирани ИКТ дейности и услуги за нуждите на МВнР да се извършват от екип от експерти на Изпълнителя, притежаващи следната професионална компетентност по предмета на поръчката:
       1. ***Ръководител проект – 1 бр.***

1. Образование: придобита образователно-квалификационна степен „магистър“ в област „Природни науки, математика и информатика“, професионално направление „Информатика и компютърни науки“ (или еквивалент) или придобита образователно-квалификационна степен „магистър“ в област „Технически науки“, професионално направление „Комуникационна и компютърна техника“ (или еквивалент), съгласно Класификатора на областите на висше образование и професионални направления, приет с Постановление № 125 на МС от 24.06.2002г.
2. Допълнителна квалификация:

* Сертификат за завършено обучение и успешно издържан изпит за прилагане на методология за управление на проекти (PMBOK, PRINCE2 или еквивалентен);
* Сертификат в областта на управлението на ИТ услуги (ITILv3 2011, ISO/IEC 20000 или еквивалентен);
* Сертификат в областта на управлението на информационната сигурност, издаден от независима международно призната организация (CISSP или еквивалентен).

1. Общ професионален опит: не по-малко от 10 г. опит в областта на информационните и/или комуникационните технологии, от които минимум 5 г. опит в областта на управлението на ИТ услуги.
2. Специфичен професионален опит: участие като ръководител на проект в най-малко 3 успешно приключени проекти в областта на предоставянето на ИТ услуги в държавната администрация и участие като ръководител на проект в най-малко 1 успешно приключен проект с предмет сходен с предмета на настоящата поръчка - Управлявани ИКТ услуги или Системна поддръжка на ИТ среда.
   * + 1. ***Проектен координатор - 1 бр.***
3. Образование: придобита образователно-квалификационна степен „магистър“ в област „Природни науки, математика и информатика“, професионално направление „Информатика и компютърни науки“ (или еквивалент) или придобита образователно-квалификационна степен „магистър“ в област „Технически науки“, професионално направление „Общо инженерство“ (или еквивалент), или придобита образователно-квалификационна степен „магистър“ в област „Социални, стопански и правни науки“, професионално направление „Администрация и управление“ (или еквивалент),съгласно Класификатора на областите на висше образование и професионални направления, приет с Постановление № 125 на МС от 24.06.2002 г.
4. Допълнителна квалификация:

* Сертификат за завършено обучение и успешно издържан изпит за прилагане на методология за управление на проекти (PMBOK, PRINCE2 или еквивалент);
* Сертификат в областта на управлението на ИТ услуги (ITILv3 2011, ISO/IEC 20000 или еквивалент).

1. Общ професионален опит: не по-малко от 5 г. опит в областта на информационните и/или комуникационните технологии, от които минимум 3 г. опит в областта на управлението на ИТ услуги.
2. Специфичен професионален опит: участие в най-малко 1 успешно приключен проект в областта на предоставянето на ИТ услуги в държавната администрация.
   * + 1. ***Ръководител технически дейности - 1 бр.***
3. Образование: придобита образователно-квалификационна степен „магистър“ в област „Природни науки, математика и информатика“, професионално направление „Информатика и компютърни науки“ (или еквивалент) или придобита образователно-квалификационна степен „магистър“ в област „Технически науки“, професионално направление „Общо инженерство“ (или еквивалент), или придобита образователно-квалификационна степен „магистър“ в област „Социални, стопански и правни науки“, професионално направление „Администрация и управление“ (или еквивалент),съгласно Класификатора на областите на висше образование и професионални направления, приет с Постановление № 125 на МС от 24.06.2002 г.
4. Допълнителна квалификация:

* Сертификат за завършено обучение и успешно издържан изпит за прилагане на методология за управление на проекти (PMBOK, Prince2 или еквивалентни);
* Сертификат в областта на управлението на ИТ услуги (сертификат по ITILv3 2011, ISO/IEC 20000 или еквивалентен).

1. Общ професионален опит: не по-малко от 10 г. опит в областта на информационните и/или комуникационните технологии, от които минимум 5 г. опит в областта на управлението на ИТ услуги.
2. Специфичен професионален опит: участие в най-малко 1 успешно приключен проект в областта на предоставянето на ИТ услуги в държавната администрация.
   * + 1. ***Експерт системно администриране и информационна сигурност - 3 бр.***
3. Допълнителна квалификация:

* Сертификат в областта на поддръжката на Microsoft базирани сървърни операционни системи (MCSE: Server Infrastructure или еквивалентен).
* Сертификат в областта на поддръжката на Linux базирани сървърни операционни системи (LPIC-2 или еквивалентен)

1. Общ професионален опит: не по-малко от 5г. опит в областта на информационните и/или комуникационните технологии, от които минимум 3г. опит в областта на управлението на ИТ услуги
2. Специфичен професионален опит: участие в най-малко 1 успешно приключен проект в областта на предоставянето на ИТ услуги в държавната администрация.
   * + 1. ***Експерт, поддръжка на пощенска инфраструктураи информационна сигурност (Еди) MCSE:Messaging) – 1 бр.***
3. Допълнителна квалификация:

* Сертификат в областта на поддръжката на Microsoft базирани сървърни инфраструктури (MCSE: Messaging или еквивалентен).

1. Общ професионален опит: не по-малко от 5г. опит в областта на информационните и/или комуникационните технологии, от които минимум 3г. опит в областта на управлението на ИТ услуги.
2. Специфичен професионален опит: участие в най-малко 1 успешно приключен проект в областта на предоставянето на ИТ услуги в държавната администрация.
   * + 1. ***Експерт мрежово администриране и информационна сигурност - 2 бр.***
3. Допълнителна квалификация:

* Сертификат в областта на управлението на мрежови инфраструктури (CCNP Service Provider или еквивалентен);
* Сертификат в областта на управлението на мрежовата сигурност (CCNP Security или еквивалентен);

1. Общ професионален опит: не по-малко от 5г. опит в областта на информационните и/или комуникационните технологии, от които минимум 3г. опит в областта на управлението на ИТ услуги.
2. Специфичен професионален опит: участие в най-малко 1 успешно приключен проект в областта на предоставянето на ИТ услуги в държавната администрация.
   * + 1. ***Експерт потребителска поддръжка и информационна сигурност –2 бр.***
3. Общ професионален опит: не по-малко от 5г. опит в областта на информационните и/или комуникационните технологии, от които минимум 3г. опит в областта на управлението на ИТ услуги.
4. Специфичен професионален опит: участие в най-малко 1 успешно приключен проект в областта на предоставянето на ИТ услуги в държавната администрация.

## Активи в ИКИ на МВнР, които са в обхвата на поръчката

### Работни станции – 650 бр.

### Сървърни системи – 65бр.

### Мрежови системи – 60 бр.

## Активи в ИКИ на МВнР, които не са в обхвата на поръчката

### Всички сървърни системи за нуждите на НВИС;

### Всички мрежови системи за нуждите на НВИС;

### Всички дискови системи за нуждите на НВИС.

## Методики

### Методика за извършване на еднократни висококвалифицирани ИКТ дейности

Необходимо е Участникът да предложи към Техническото предложение документ „Методика за извършване на еднократни висококвалифицирани ИКТ дейности“, в който да са засегнати детайлно:

* Документиране на ИКИ;
* Анализиране и преконфигуриране на Активна директория;
* Анализиране и преконфигуриране на безжични мрежи;
* Инвентаризиране на приложни системи;
* Първоначално сканиране за технически уязвимости и прилагане на мерки за отстраняване на открити несъответствия;
* Анализиране на работни станции за наличие на зловреден софтуер;
* Анализиране на сървърни системи за наличие на зловреден софтуер;
* Реализиране на IDS функционалност;
* Оценяване на рисковете в ИКИ.

### Методика за предоставяне на регулярни висококвалифицирани ИКТ услуги

Необходимо е Участникът да предложи към Техническото предложение документ „Методика за предоставяне на регулярни висококвалифицирани ИКТ услуги“, в който да са засегнати детайлно:

* Сканиране за техническите уязвимости и прилагане на мерки за отстраняване на откритите несъответствия;
* Преглед на работните станции за наличие на зловреден софтуер;
* Преглед на сървърните системи за наличие на зловреден софтуер;
* Наблюдение на реализираната IDS функционалност и предприемане на проактивни мерки;
* Експертна помощ на място и реакция при инциденти.

### Методика за осигуряване на защита на мрежовия трафик на МВнР

Необходимо е Участникът да предложи към Техническото предложение документ „Методика за осигуряване на защита на мрежовия трафик на МВнР“, в който да са засегнати детайлно:

* Защита от зловреден код в операционните системи;
* Защита от Distributed Denial of Service (DDoS).

## Отчитане

Необходимо е Изпълнителят да предоставя3 (три) месечни доклади за отчитане на дейностите или услугите по проекта, които да съдържат:

* Информация за извършените дейности и предоставените услуги;
* Информация за състоянието на ИКИ и;
* Препоръки за постиганеи поддържане на ниски нива на информационните рискове.

Докладите за отчитане на дейностите и услугите по проекта се приемат от Възложителя с приемо-предавателен протокол.

# **Извършване на еднократни висококвалифицирани ИКТ дейности**

Всички еднократни висококвалифицирани ИКТ дейности са свързани с постигане на ниски нива на информационните рискове, които да бъдат поддържани впоследствие чрез предоставяните регулярни ИКТ услуги и гарантиране на поверителността, цялостността и наличността на трансферираната, обработваната и съхраняваната информацията в ИКИ на МВнР.

Необходимо е всички описани по-долу еднократни ИКТ дейности да бъдат изпълнени в срок до 3 (три) месеца, считано от датата на подписване на договор с Изпълнителя, в Етап 1 от проекта.

## Документиране на ИКИ на физическо ниво

Необходимо е Изпълнителят да извърши цялостно обследване на съществуващата ИКИ на физическо ниво на МВнР и да изготви детайлна техническа документация, която да бъде поддържана до края на проекта. Необходимо е документацията да съдържа:

### Физическата топология на изградената комуникационна мрежа:

* + - * Топология на използваните комуникационни трасета;
      * Разположение и вид на мрежовите устройства;
      * Разположение и вид на крайните устройства - сървъри, работни станции, комуникационно оборудване и периферни устройства.

### Използвани сървърни помещения:

* + - * Системи за контрол на достъпа;
      * Системи за осигуряване на параметрите на обкръжаващата среда;
      * Системи за пожаро-известяване/гасене;
      * Системи за осигуряване на непрекъсваемо захранване.

## Документиране на ИКИ на логическо ниво

Необходимо е Изпълнителят да извърши цялостно обследване на съществуващата ИКИ на логическо ниво на МВнР и да изготви детайлна техническа документация, която да бъде поддържана до края на проекта. Необходимо е документацията да съдържа:

### Физически канали за връзка от МВнР към външни организации и/или доставчици:

* + - * Физическа свързаност към доставчик/ици на Интернет;
      * Физическа свързаност към ЕЕСМ на ДА;
      * Други връзки - радиорелейни връзки, сателитни и/или други комуникации.

### Физически връзки между отделните устройства;

### HLD, LLD и схеми;

### Конфигурации на:

* + - * Маршрутизатори;
      * Защитни стени;
      * Комутатори в ядрото на мрежата;
      * Комутаторите в слоя за достъп на мрежата.

### Политики за:

* + - * Управление на комуникационната инфраструктура – виртуални мрежи за управление на устройствата, контрол на достъпа;
      * Достъп до сървърните системи;
      * Отдалечен достъп.

### Процедури за създаване на резервни копия на конфигурационните файлове на отделните устройства и проследяване на промени по конфигурациите.

## Анализиране и преконфигуриране на Активна директория (MS AD)

Необходимо е Изпълнителят да анализира и преконфигурира Активната директория и домейн контролерите на МВнР, с цел постигане на ниски нива на информационните рискове за участващите в Активната директория компоненти - работни станции, сървъри и периферни устройства. Необходимо е да се извършат следните дейности:

* + - * Анализ на потребителите с административни и/или системни права;
      * Анализ на възникналите и потенциалните проблеми при репликиране между домейн контролерите;
      * Анализ на състоянието на дялове за данни на Активната директория;
      * Анализ и преконфигуриране на топологията на използваната Активна директория, в т.ч. топология на Forest ниво, Domain ниво и репликациите между домейн контролерите;
      * Анализ и преконфигуриране на инсталираният софтуер върху домейн контролерите на Активната директория;
      * Анализ и преконфигуриране на груповите политики в Активната директория;
      * Преконфигуриране на домейн контролерите и/или обновяването им до по-нови версии;
      * Преконфигуриране на политики за сигурност за потребителите на Активната директория.

## Анализиране и преконфигуриране на безжични мрежи

Необходимо е Изпълнителят да анализира и преконфигурира безжичните мрежи на МВнР, с цел постигане на ниски нива на информационните рискове. Необходимо е да се извършат следните дейности:

* + - * Анализ на потребителите имащи право за ползване на безжични комуникации;
      * Анализ на налични несанкционирани точки за достъп;
      * Анализ и преконфигуриране на протоколи за сигурност;
      * Анализ и преконфигуриране на достъпа през безжичните мрежи.

## Инвентаризиране на приложните системи

Необходимо е Изпълнителят да инвентаризира всички приложни системи, работещи в МВнР. Необходимо е да се извършат следните дейности:

* + - * Изготвяне на списък на всички приложни системи и свързаните с тях ИТ услуги;
      * Изготвяне на техническа спецификация за всяка приложна система;
      * Изготвяне на описание на техническите изисквания за всяка приложна система;
      * Разработване на политики за резервиране на информацията обработвана чрез всяка приложна система.

## Първоначално сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия

Необходимо е Изпълнителят да сканира за технически уязвимости всички работещи в МВнР информационни системи – мрежови, сървърни и потребителски. Необходимо е тестът за техническа уязвимост да представлява активен комплекс от дейности, които да се извършват чрез сканиране с автоматизирани инструменти (ползващи база данни от Network Vulnerability Tests (NVTs)) и прилагане на експертни неавтоматизирани методи. Необходимо е процесът на тестване да обхваща публично достъпните и локалните информационни ресурси на МВнР и да извършва проверка за наличие на Common Vulnerabilities and Exposures (CVE), регистрирани в глобалните бази данни. Необходимо е всяко открито несъответствие да се анализира и оценява посредством Common Vulnerability Scoring System (CVSS), която дава информация за характеристиките на уязвимостите и формира числови оценки на критичността им.

Необходимо е да се извършат следните дейности:

* + - * Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички публично достъпни ИТ услуги;
      * Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички ИТ ресурси в локалните мрежи.

## Анализиране на работните станции за наличие на зловреден софтуер

Необходимо е Изпълнителят да анализира всички работни станции за зловреден софтуер и да изготви план за преконфигуриране, надстройване, преинсталиране или деинсталиране на приложения и/или операционни системи, който да бъде реализиран в рамките на предоставяне на услуги в Етап 2 от проекта.

Необходимо е да се извършат следните дейности:

* + - * Анализиране за компютърни вируси;
      * Анализиране за известни RootKits - механизми и техники, чрез които зловредни програми, вкл. компютърни вируси, шпионски програми и троянски коне, се опитват да се скрият от антивирусни програми и други приложения за сигурност;
      * Анализиране за участие на работните станции в botnets;
      * Анализиране за инсталиран софтуер, без знанието на потребителя, който събира лична информация за него (spyware), в т.ч. софтуер за събиране на пароли (keylogger);
      * Анализиране за софтуер, който управлява рекламни съобщения (adware);
      * Изготвяне на общ план за преконфигуриране, надстройване, преинсталиране или деинсталиране на приложения и/или операционни системи.

## Анализиране на сървърни системи за наличие на зловреден софтуер

Необходимо е Изпълнителят да анализира всички сървърни системи за зловреден софтуер и да изготви план за преконфигуриране, надстройване, преинсталиране или деинсталиране на приложения и/или операционни системи, който да бъде реализиран в Етап 2 от проекта.

Необходимо е да се извършат следните дейности:

* + - * Анализиране за компютърни вируси;
      * Анализиране за известни RootKits - механизми и техники, чрез които зловредни програми, вкл. компютърни вируси, шпионски програми и троянски коне, се опитват да се скрият от антивирусни програми и други приложения за сигурност;
      * Анализиране за участие на сървърните системи в botnets;
      * Анализиране за инсталиран софтуер, без знанието на системните администратори, който събира лична информация (spyware), в т.ч. софтуер за събиране на пароли (keylogger);
      * Анализиране за софтуер, който управлява рекламни съобщения (adware);
      * Изготвяне на общ план за преконфигуриране, надстройване, преинсталиране или деинсталиране на приложения и/или операционни системи.

## Реализиране на IDS функционалност

Необходимо е Изпълнителят да идентифицира и отстрани познатите зловредни софтуери в МВнР, като наблюдава и изолира нетипичния мрежови трафик – изходящ и входящ, чрез реализиране на IDS функционалност, която пасивно да регистрира изградените мрежови връзки между граничната защитна стена и агрегиращите комутатори в мрежата на МВнР.

Необходимо е да се извършат следните дейности:

* + - * Инсталиране, конфигуриране и управление на специализирано хардуерно устройство, собственост на Изпълнителя, което да работи в IDS режим, пасивно регистрирайки изградените мрежови връзки между граничната защитна стена и агрегиращите комутатори в мрежата на МВнР;
      * Изолиране на нетипичния мрежови трафик – изходящ и входящ.

## Оценяване на рисковете в ИКИ

Необходимо е Изпълнителят да изготви оценка на риска, която да съдържа идентифицирани, анализирани и оценени рискове, за всеки от които е направена конкретна препоръка за постигане и поддържане на ниски нива на информационните рискове, която да бъде реализирана в Етап 2 от проекта.

Необходимо е оценката на риска да съдържа:

* + - * Актив;
      * Местонахождение;
      * Стойност на актива;
      * Заплаха;
      * Уязвимо място;
      * Въздействие на заплахата;
      * Вероятност за инцидент;
      * Честота на инцидент;
      * Оценка на риска;
      * Категория на риска;
      * Препоръка за постигане и поддържане на ниски нива на информационните рискове.

## Първоначално конфигуриране на ИКИ оборудване, при необходимост

Необходимо е Изпълнителят да осигури висококвалифицирани експерти, които при необходимост да извършват първоначално конфигуриране на ИКИ оборудване, собственост на МВнР, и мигриране на ИТ услугите в ИКИ на МВнР към него.

При необходимост да се извършат следните дейности:

* + - * Конфигуриране на гранични комутатори;
      * Конфигуриране на гранични маршрутизатори;
      * Конфигуриране на защитни стени;
      * Конфигуриране на опорни комутатори;
      * Конфигуриране на SAN комутатори;
      * Конфигуриране на комутатори за клиентски достъп;
      * Конфигуриране на сървърни системи.

# **Предоставяне на регулярни висококвалифицирани ИКТ услуги**

Всички регулярни висококвалифицирани ИКТ услуги са свързани с поддържане на ниски нива на информационните рискове и гарантиране на поверителността, цялостността и наличността на трансферираната, обработваната и съхраняваната информацията в информационната и комуникационната инфраструктура (ИКИ) на МВнР. Регулярността на услугите е с период 1 (един) месец.

Необходимо е всички описани по-долу регулярни ИКТ услуги да бъдат изпълнявани в срок от 21 (двадесет и един) месеца, в Етап 2 от проекта, считано от датата на приключване на еднократните ИКТ дейности в Етап 1 на проекта.

## Сканиране за техническите уязвимости и прилагане на мерки за отстраняване на откритите несъответствия

Необходимо е Изпълнителят да сканира за технически уязвимости всички работещи в МВнР информационни системи – мрежови, сървърни и потребителски. Необходимо е тестът за техническа уязвимост да представлява активен комплекс от дейности, които да се извършват чрез сканиране с автоматизирани инструменти (ползващи база данни от Network Vulnerability Tests (NVTs)) и прилагане на експертни неавтоматизирани методи. Необходимо е процесът на тестване да обхваща публично достъпните и локалните информационни ресурси на МВнР и да извършва проверка за наличие на Common Vulnerabilities and Exposures (CVE), регистрирани в глобалните бази данни. Необходимо е всяко открито несъответствие да се анализира и оценява посредством Common Vulnerability Scoring System (CVSS), която дава информация за характеристиките на уязвимостите и формира числови оценки на критичността им.

Необходимо е да се предоставят регулярно следните услуги:

* + - * Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички публично достъпни ИТ услуги;
      * Сканиране за технически уязвимости и прилагане на мерки за отстраняване на откритите несъответствия за всички ИТ ресурси в локалните мрежи.

## Преглед на работните станции за наличие на зловреден софтуер

Необходимо е Изпълнителят да анализира всички работни станции за зловреден софтуер и да преконфигурира, надстройва, преинсталира или деинсталира приложения и/или операционни системи, включително и съгласно изготвеният план в Етап 1 на проекта.

Необходимо е да се предоставят регулярно следните услуги:

* + - * Анализиране за компютърни вируси;
      * Анализиране за известни RootKits - механизми и техники, чрез които зловредни програми, вкл. компютърни вируси, шпионски програми и троянски коне, се опитват да се скрият от антивирусни програми и други приложения за сигурност;
      * Анализиране за участие на работните станции в botnets;
      * Анализиране за инсталиран софтуер, без знанието на потребителя, който събира лична информация за него (spyware), в т.ч. софтуер за събиране на пароли (keylogger);
      * Анализиране за софтуер, който управлява рекламни съобщения (adware).

## Преглед на сървърните системи за наличие на зловреден софтуер

Необходимо е Изпълнителят да анализира всички сървърни системи за зловреден софтуер и да преконфигурира, надстройва, преинсталира или деинсталира приложения и/или операционни системи, включително и съгласно изготвеният план в Етап 1 на проекта.

Необходимо е да се предоставят регулярно следните услуги:

* + - * Анализиране за компютърни вируси;
      * Анализиране за известни RootKits - механизми и техники, чрез които зловредни програми, вкл. компютърни вируси, шпионски програми и троянски коне, се опитват да се скрият от антивирусни програми и други приложения за сигурност;
      * Анализиране за участие на сървърните системи в botnets;
      * Анализиране за инсталиран софтуер, без знанието на системните администратори, който събира лична информация (spyware), в т.ч. софтуер за събиране на пароли (keylogger);
      * Анализиране за софтуер, който управлява рекламни съобщения (adware).

## Наблюдение на реализирана IDS функционалност и предприемане на проактивни мерки

Необходимо е Изпълнителят да наблюдава и управлява реализираната IDS функционалност, която пасивно регистрира изградените мрежови връзки между граничната защитна стена и агрегиращите комутатори в мрежата на МВнР.

Необходимо е да се предоставят регулярно следните услуги:

* + - * Наблюдение и управление на специализирано хардуерно устройство, което работи в IDS режим, пасивно регистрирайки изградените мрежови връзки между граничната защитна стена и агрегиращите комутатори в мрежата на МВнР;
      * Наблюдаване и изолиране на нетипичния мрежови трафик – изходящ и входящ.

## Експертна помощ на място и реакция при инциденти

Необходимо е Изпълнителят да осигури минимум двама експерта, които в рамките на работното време на ВЪЗЛОЖИТЕЛЯ, от 09:00 часа до 17:30 часа, да се ангажират с предоставяне на експертна помощ на място и реакция при инциденти свързани със сигурността.

## Наблюдение и управление на мрежово оборудване

Необходимо е Изпълнителят да осигури висококвалифицирани експерти, които да наблюдават и управляват мрежовото оборудване на ИКИ на МВнР.

Необходимо е да се предоставят регулярно следните услуги:

* + - * Наблюдение на мрежово оборудване;
      * Управление на мрежово оборудване.

## Прилагане на препоръки от оценката на риска

Необходимо е Изпълнителят да приложи направените препоръки за постигане и поддържане на ниски нива на информационните рискове.

## Конфигуриране на ИКИ оборудване, при необходимост

Необходимо е Изпълнителят да осигури висококвалифицирани експерти, които при необходимост да извършват конфигуриране на ИКИ оборудване, собственост на МВнР, и мигриране на ИТ услугите в ИКИ на МВнР към него.

При необходимост да се извършат следните дейности:

* + - * Конфигуриране на гранични комутатори;
      * Конфигуриране на гранични маршрутизатори;
      * Конфигуриране на защитни стени;
      * Конфигуриране на опорни комутатори;
      * Конфигуриране на SAN комутатори;
      * Конфигуриране на комутатори за клиентски достъп;
      * Конфигуриране на сървърни системи.

# **Осигуряване на защита на мрежовия трафик на МВнР**

Защитата на мрежовия трафик е свързана с постигане и поддържане на ниски нива на информационните рискове и гарантиране на поверителността, цялостността и наличността на трансферираната, обработваната и съхраняваната информацията в информационната и комуникационната инфраструктура (ИКИ) на МВнР.

Необходимо е всички описани по-долу ИКТ дейности и услуги да бъдат изпълнявани в срок от 24 (двадесет и четири) месеца, считано от датата на започване изпълнението на договора с Изпълнителя, в Етап 3 от проекта.

## Защита от зловреден код в операционните системи

Необходимо е Изпълнителят да защити от зловреден код в операционните системи всички ресурси на МВнР, като открие, премахне и възпрепятства дълбоко прикрит зловреден код в операционните системи, който комуникира с отдалечени сървъри за контрол (C&C), с цел събиране на информация или генериране на зловреден трафик.

Необходимо е да се извършат следните дейности:

* + - * Откриване на зловреден трафик чрез познати сигнатури, които се обновяват ежечасно;
      * Анализиране на аномалии в трафика и извършване на корелация в реално време.

## Защита от Distributed Denial of Service (DDoS)

Необходимо е Изпълнителят да защити от зловреден код в операционните системи всички ресурси на МВнР, като предпази публичните ИТ услуги на МВнР от DDoS.

Необходимо е да се извършат следните дейности:

* + - * Анализиране на входно-изходния мрежови трафик, като се следи за комуникация към потенциални C&C центрове, списъка за който е генериран от детектори, разположени в ключови Интернет доставчици по целия свят;
      * В случай на DDoS атака, пренасочване на входно-изходния мрежови трафик през Интернет базиран скръбинг център.