ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ОПЕРАТИВНА ПРОГРАМА ДОБРО УПРАВЛЕНИЕ

ПРОУЧВАНЕ И АНАЛИЗ НА ЗАКОНОДАТЕЛСТВОТО, ИМАЩО ОТНОШЕНИЕ КЪМ КИБЕРСИГУРНОСТТА В ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

Дейност 1 от проект № BG05SFOP001-2.025-0074-C01“ Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран по ОПДУ 2014-2020

Бенефициент: Фондация „Ресурсен център“
Партньор 1: Община Дупница
Партньор 2: Фондация „Икономика и право“

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

СЪДЪРЖАНИЕ:

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

I. Увод:

Основна цел на законодателствата на държавите-членки на ЕС и в частност на България в последните няколко години е постигането на високо общо ниво на мрежова информационна сигурност във всички сегменти на киберпространството, повишаване на сигурността на националните и на частните мрежи и информационни системи, и постигането на информационна сигурност на всички нива – граждани, държавни и бизнес организации, доставчици и потребители на услуги. В условията на нарастваща и необратима дигитална зависимост, дефицитите в мрежовата и информационна сигурност водят до компрометиране на основни услуги, спиране на дейности и загуби, кражба или изтичане на лични данни.

Именно с цел повишаване на защитата постоянно се извършва анализ на действащото законодателство, неговата актуалност и пропорционалност на съществуващите заплахи.

Електронното управление в България се превърна в постоянен приоритет в последните години, като това налага гарантиране на сигурен и защитен достъп до електронни административни услуги за гражданите и бизнеса. В областта на административните услуги най- уязвим е сектора със защита на личните данни, тъй като администрациите боравят, разполагат, съхраняват, обработват огромно количество лични данни, което ги превръща в най-предпочитаната област за кибератаки и киберпрестъпления. Именно това налага осигуряването на защитата на лични данни и чувствителна информация от всеки вид и то на високо ниво.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

1. Понятие за киберсигурност

Киберсигурността има легална дефиниция, дадена в чл. 2 на Закона за киберсигурност като тя се определя като състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.

Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана.

Мрежова и информационна сигурност се определя като способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.

България участва активно във формирането и осъществяването на политиките за киберсигурност в рамките на ЕС и НАТО и се стреми към постигане на киберустойчивост на цялото общество и държава.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

II. Нормативна база:

II.1. Национално законодателство:

- **Закон за киберсигурност:**

Законът за киберсигурност (Обн. ДВ. бр.94 от 13 Ноември 2018г., изм. ДВ. бр.69 от 4 Август 2020г., изм. и доп. ДВ. бр.85 от 2 Октомври 2020г., изм. и доп. ДВ. бр.15 от 22 Февруари 2022г., изм. ДВ. бр.25 от 29 Март 2022г.) е изработен в изпълнение на ангажиментите на Република България като държава- членка на Европейския съюз да въведе в националното си законодателство разпоредби и да създаде организация за изпълнението на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 06.07.2016 г относно мерки за високо общо ниво на сигурност на мрежите и информационните системи на съюза.

Законът за киберсигурност разглежда:

– организацията, управлението и контрола на киберсигурността, определянето на компетентните органи в областта на киберсигурността, както и техните функции и правомощия, регламентирането на дейностите по предприемане на необходимите мерки за постигане на високо общо ниво на сигурност на мрежите и информационните системи, като един основен стълб на киберсигурността, така че да се подобри функционирането на вътрешния пазар;

– създаване на институционалната рамка в областта на киберсигурността, превенцията и противодействието на кибер атаките, насочена към по-голяма ефективност и по-добра координация между съществуващите органи и звена в публичната администрация;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

– предвижда се създаването на нови компетентни органи, като Национално единно звено за контакт, регламентира се управлението и организацията на националната система за киберсигурност, Националния координатор по киберсигурност, секторни екипи за реакция при инциденти в киберсигурността – ЕРИКС, както и Национален ЕРИКС (създаден от председателя на Държавна агенция „Електронно управление“, понастоящем Министерство на електронното управление), предвижда се и създаването на Националната стратегия за киберсигурност, регламентират се въпросите за междуинституционална взаимосвързаност и сътрудничество;

– регулацията на мрежовата и информационна сигурност на административните органи, изискванията към тях да осигуряват и отговарят за мрежовата и информационната сигурност на използваните от тях информационни системи, също така зискванията и стандартите за сигурност, на които трябва да отговарят информационните системи за въвеждане, изпращане, обработка, достъп, обмен, съхраняване и архивиране на данни, както и общите мерки за сигурност, които трябва да предприемат;

– статута и функционирането на операторите на съществени услуги (ОСУ);

– националните компетентни органи (НКО), които разполагат с всички необходими правомощия и средства за оценяване на това дали операторите на съществени услуги изпълняват задълженията си;

– статута и функционирането на доставчиците на цифрови услуги (ДЦУ).

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **НАРЕДБА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ**

С наредбата се уреждат:

1. изисквания за минималните мерки за мрежова и информационна сигурност;

2. препоръчителни мерки за мрежова и информационна сигурност;

3. правила за извършване на проверките за съответствие с изискванията на тази наредба;

4. редът за водене, съхраняване и достъп до регистъра на съществените услуги по чл. 6 от Закона за киберсигурност;

5. образец на уведомленията за инциденти

Наредбата е приета на основание чл. 3, ал. 2 от Закона за киберсигурност с Постановление на Министерски съвет № 186 от 19.07.2019 г.

Наредбата се прилага за администативните органи както и за други субекти, но за целите на настоящото изложение ще бъде акцентирано върху административните органи.

- **ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ (ЗЕУ):**

Със Закона за електронното управление се прехвърлят всички правомощия, които дотогава е упражнявал председателят на Държавната агенция "Електронно управление" (ДАЕУ) в областта на електронното управление и

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

правомощията в областта на информационните технологии на министъра на електронното управление. Със закриването на ДАЕУ следва и преминаването на дирекция „Информационни технологии“ от Министерство на информационните технологии и съобщенията към Министерството на електронното управление.

Основната цел на ЗЕУ е да уреди правомощията и функциите на министъра на електроното управление като орган за осъществяване на политиката за електронно управление и в областта на информационното общество и информационните технологии във взаимодействие с другите органи на изпълнителната власт.

Със закона се уреждат обществените отношения между административните органи, свързани с работата с електронни документи и предоставянето на административни услуги по електронен път, както и обмена на електронни документи между административните органи.

Законът въвежда предоставянето на електронни административни услуги, както и задължението на администрациите да приемат документи по електронен път и да издават документи по електронен път.

Административните органи, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, са длъжни да предоставят всички услуги в рамките на своята компетентност и по електронен път, освен ако закон предвижда особена форма за извършване на отделни действия или издаване на съответни актове.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Законът изисква административните органи да използват информационни системи, които да съответстват на изискванията за оперативна съвместимост и мрежова и информационна сигурност по ЗЕУ и по Закона за киберсигурност.

- **ЗАКОН ЗА ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ**

Законът за електронната идентификация поставя нормативни изисквания за сигурност.

Администраторите на електронна идентичност, съответно центровете за електронна идентификация създават и поддържат вътрешни процедури за сигурност, съгласно които осъществяват дейността си.

Процедурите за сигурност трябва да съответстват на изискванията за управление на информационната сигурност, определени с правилника за прилагане на закона.

Процедурите за сигурност съдържат най-малко:

1. оценка на риска;

2. управленски мерки за сигурност;

3. мерки за информационна сигурност;

4. разполагаеми финансови средства или застраховки;

5. изисквания за надеждност на персонала;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

6. мерки за осигуряване на защита и за ограничаване на достъпа до отделни устройства и помещения;

7. мерки за осигуряване на защита срещу непозволен достъп до информационните системи;

8. мерки за осигуряване на защита срещу непозволени промени;

9. план за действие при събития, съставляващи непреодолима сила, и при последващо възстановяване на дейността.

Процедурите за сигурност не са публични. Достъп до тях имат само министърът на вътрешните работи и лицата по чл. 35 от Закона за електронната идентифкация.

- **НАРЕДБА ЗА ОБЩИТЕ ИЗИСКВАНИЯ КЪМ ИНФОРМАЦИОННИТЕ СИСТЕМИ, РЕГИСТРИТЕ И ЕЛЕКТРОННТЕ АДМИНИСТРАТИВНИ УСЛУГИ**

Наредбата е приета с Постановление на Министерски съвет (ПМС) № 3 от 09.01.2017 г.

Наредбата поставя изисквания пред ръководителите на администрациите да извършват оценка на информационната сигурност и защитата на личното пространство с оглед въвеждането на електронната административна услуга.

Също така Наредбата очертава общи изисквания към информационните системи и софтуерните компоненти:

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Всички информационни системи и софтуерните компоненти в администрацията, включително и регистри, интернет страници, вътрешни информационни системи, потребителски интерфейси към съществуващи системи, системи за предоставяне на електронни административни услуги и за електронен документооборот, трябва да отговарят на изискванията на Наредбата.

Интернет страниците на администрациите трябва отговарят на правилата за институционална идентичност, определени от министъра на електронното управление. Съществува разработен през Единен портал за достъп до електронни административни услуги (ЕПДЕАУ) - Държавна агенция "Електронно управление" единен шаблон за интернет страница на община: https://staging.egov.bg/wps/portal/template-municipality/municipality-name/home/

Наредбата въвежда изискване съответният ръководител да посочи длъжностно лице, което да осигурява автоматизираното създаване на резервни копия на всички данни и електронни документи най-малко всеки ден.

Всички доставчици на електронни административни услуги са длъжни да използват удостоверения за автентичност на уебсайтове, на които са разположени официалните интернет страници или на които са разположени информационните системи, чрез които се предоставят електронни административни услуги.

За осигуряване на сигурен достъп до интернет страниците и другите услуги в интернет посредством наименование на домейн трябва да се използва услугата DNSSec (Domain Name Service - Security - Сигурна услуга за името на домейна), основана на

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

препоръки RFC 2535 и 2931, приети от IETF (The Internet Engineering Task Force - Целева група за интернет инженеринг) през март 1999 г.

II.2 Европейско законодателство**:**

- **ЕС - ДИРЕКТИВА (ЕС) 2016/1148 (МИС):**

Директива (ЕС) 2016/1148 е първото всеобхватно законодателство в областта на мрежовата и информационна сигурност (МИС) на ниво ЕС и предоставя хармонизирана правна основа за борба с кибер инцидентите в целия ЕС. Основните ѝ цели са: 1. да разреши проблема с недостатъчното равнище на защита срещу инциденти, рискове и заплахи в областта на мрежовата и информационната сигурност в ЕС, което възпрепятства правилното функциониране на вътрешния пазар; 2. да способства за преодоляването на нарастващия брой инциденти, както и с цел постигане на високо общо ниво на мрежите и информационните системи във всички сегменти на кибер пространството и на всички нива – държава, граждани, фирми и бизнес организации, доставчици и потребители на услуги.

Директивата се отменя считано от 18.10.2024 г. като от този момент нататък започва да се прилага Директива (ЕС) 2022/2555 на Европейския парламетн и на Съвета от 14.12.2022 г относно мерките за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/172 и за отмяна на Директива (ЕС) 2016/1148.

Въпреки че ще бъде отменена считано от 18.10.2024 г Директива (ЕС) 2016/1148 е основополагаща за мрежовата и информационната сигурност в рамките на целия Европейски съюз, като е послужила за основа и на приетите и действащи и към момента

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

национални законови и подзаконови нормативни актове в областта на киберсигурността и мрежовата и информационна сигурност.

- **Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)**

Общият регламент относно защитата на данните (ОРЗД), по- известен с английското съкращение GDPR (General Data Protection Regulation) има за своя основна цел да гарантира на гражданите контрол върху техните лични данни. Особеност на този Регламент е, че разпростира действието си и върху субекти извън ЕС и Европейската икономическа зона (ЕИЗ), когато се касае за обработка на лични данни на граждани на ЕС.Общият регламент относно защитата на данните поставя редица изисквания, на които държавите-членки следва да отговарят във връзка със защитата и сигурността на личните данни на европейските граждани, включително и в областта на мрежовата и информационна сигурност.

- **Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации)**

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Директивата определя правила, които гарантират сигурността при обработката на лични данни, уведомяването за нарушения на сигурността на личните данни и конфиденциалния характер на комуникациите. Тя също така забранява нежеланите съобщения, когато потребителят не е дал съгласието си.

Доставчиците на електронни комуникационни услуги следва да гарантират, че достъп до личните данни имат само упълномощени лица; да защитят личните данни от унищожаване, загуба или случайна промяна, както и от други незаконни или неоторизирани форми на обработка; както и да осигурят изпълнението на политика на сигурност относно обработката на личните данни.

Директивата е изменена с Директива 2009/163/ЕО на Европейския парламент и на съвета от 25.11.2009 г., като е дадена дефиниция за нарушение на сигурността на личните данни – това е нарушение на сигурността, което води до случайно или незаконно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, предавани, съхранявани или по друг начин обработвани във връзка с предоставянето на обществено достъпна електронна съобщителна услуга в Общността.

II.3 Цели на уредбата:

Уредбата на европейско и национално ниво има за цел да бъдат утвърдени общи понятия в киберсигурността, да се определят компетентни органи вътре в държавата, а и такива отговарящи на международно ниво, да се конкретизират субектите в обсега на закона и да се създаде подготвеност в ключовите за държавата сектори с цел едно работещо сътрудничество, адекватна реакция и бърз отговор в случай на кибер инциденти. Уредбата въвежда нов подход, който се основава на принципа на взаимна

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

координация, сътрудничество, както вътре в страната, така и на европейско ниво.

По-високото ниво на сигурност подобрява доверието на гражданите в онлайн средата и те могат изцяло да се възползват от възможностите на цифровия свят (напр. социални медии, електронно правителство, електронно обучение, електронно здравеопазване).

Основната цел на националното законодателство е постигането на високо общо ниво на мрежова информационна сигурност във всички сегменти на киберпространството, повишаване на сигурността на националните и на частните мрежи и информационни системи, и постигането на информационна сигурност на всички нива – граждани, държавни и бизнес организации, доставчици и потребители на услуги. В условията на нарастваща и необратима дигитална зависимост, дефицитите в МИС водят до компрометиране на основни услуги, спиране на дейности и загуби, кражба или изтичане на лични данни.

III. Изисквания, определени с Директива 2016/1148:

III. 1. Изискване за национална стратегия:

В Република България е приета Национална стратегия за киберсигурност „Киберустойчива Бълария 2020“, която е синхронизирана със Стратегията на ЕС за киберсигурност от 2013 г., и е съобразена с изискванията на Директивата на ЕС за мрежова и информационна сигурност (Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза).

Националната стратегия за киберсигурност е стратегическа рамка на политиката

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

за киберсигурност на Република България и включва:

1.цели, принципи и приоритети;

1. области на действие и мерки:

- система за киберсигурност;
- мрежова и информационна сигурност;
- противодействие на киберпрестъпността;
- киберотбрана;
- киберразузнаване;

1. взаимодействие между държава, бизнес и общество;,

2. развитие и подобряване на регулаторната рамка;

3. повишаване на осведомеността, знанията и компетентностите;

4. стимулиране на изследванията и иновациите в областта на киберсигурността;

5. международно взаимодействие;

6. кибердипломация;

7. взаимодействие на техническо, оперативно и стратегическо (политическо) ниво.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

В периода на изпълнение на Стратегията е налице увеличаване на броя постъпили сигнали за извършени компютърни престъпления, което увеличение е четири пъти повече в сравнение с предходния период. Констатира се усложняване на киберкартината в страната, което се потвърждава и от увеличението с 45 % на броя на получените сигнали за киберинциденти за тригодишен период, като тези с висок приоритет нарастват с 29 %.

Значителен обществен отзвук предизвикаха киберинциденти с прекъсване на услугите на Търговския регистър през м. август 2018 г., както и кибератаката срещу информационната система на НАП през м. юли 2019 г. През 2020 г два фактора оказват съществено влияние върху картината на застрашеност в киберпространството - въздействието на пандемията COVID - 19 и нарастващите възможности на извършителите на киберзаплахи. Наблюдаваните съществени промени през 2019 и 2020 г. в киберкартината на заплахите и рисковете за киберсигурността в национален и общоевропейски план (вкл. масирани кибератаки и връзка между кибератаки, хибридни заплахи и тероризъм, опити за намеса в демократични процеси и пряко в избори) налагат съответни промени в Националната стратегия за киберсигурност “Киберустойчива България 2020”.

Това дава обосновка за актуализация на националната стратегия „Киберустойчива България 2023 г“, като внесените промени са съобразени изцяло с приетата Стратегия на ЕС за Съюза на сигурност с обхват 2020- 2025 г[1]

В Стратегията на ЕС за Съюза за сигурност са възприети четири стратегически

[1]https://eur-lex.europa.eu/legal-content/BG/TXT/?qid=1596452256370&uri=CELEX%3A52020DC0605

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

приоритета:

- изграждането на способности и капацитет за осигуряване на среда на сигурност,
- ефективното справяне с киберпрестъпността,
- широка осведоменост на обществото
- изграждане на силна европейска екосистема на сигурност и в частност, сътрудничеството и обмена на информация

През 2022 г. 87.3% от домакинствата в България имат достъп до интернет в домовете си, което е с 3.8 процентни пункта повече в сравнение с предходната 2021 година.

79.0% от лицата на възраст между 16 и 74 навършени години използват интернет всеки ден или поне веднъж седмично на работа, вкъщи или на друго място, а 61.2% се възползват от ресурсите на глобалната мрежа по няколко пъти на ден.[2]

По данни на НСИ значително е нарастнал броят на лицата, които използват интернет с цел взаимодействие с публични институции, като за 2022 г[3] той достига общо 26.4 %, като тенденцията е този процент да нараства все повече.

[2]Изследване на НСИ– https://www.nsi.bg/sites/default/files/files/pressreleases/ICT_hh2022_JMM9789.pdf
[3]Данни от НСИ - https://www.nsi.bg/bg/content/2824/%D0%BB%D0%B8%D1%86%D0%B0-%D0%B8%D0%B7%D0%BF%D0%BE%D0%BB%D0%B7%D0%B2%D0%B0%D1%89%D0%B8-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%81-%D1%86%D0%B5%D0%BB-%D0%B2%D0%B7%D0%B0%D0%B8%D0%BC%D0%BE%D0%B4%D0%B5%D0%B9%D1%81%D1%82%D0%B2%D0%B8%D0%B5-%D1%81-%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D1%87%D0%BD%D0%B

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Киберпространството предоставя големи възможности за развитие, но води и до нарастваща и необратима цифрова зависимост на основните функции и дейности в обществото. Злонамерени или неумишлени действия могат да доведат до нарушаване работата на системите за управление и устройствата, свързани с критичната инфраструктура и възпрепятстване на нормалното им функциониране. Заплахите и рисковете в киберпространството са трудни за дефиниране поради сложността на определяне на източника на въздействие, целите и мотивите, бързото ескалиране на заплахата, трудно предвидимите перспективи за развитие, сложността и интензивността на съвременните комуникационни и информационни процеси, динамиката на логическите и физическите връзки и неопределеността на процесите. Идентифицирането, защитата и минимизирането на тези заплахи и рискове не са традиционни и изискват нова култура на взаимодействие между участниците в киберпространството.

Националната стратегия предвижда до 2023 г България да постигне киберустойчивост и да изгради функционираща, надеждна и сигурна цифрова инфраструктура за отключване на пълния потенциал на цифровите технологии за цифрова трансформация на всички ключови сектори.

В съответствие със стратегиите и политиките на Европейския съюз и НАТО на челна позиция сред стратегичеките цели е поставено постигането на киберустойчивост на цялото общество и държава, изразяващо се в ефективна защита срещу и адекватна реакция на кибератаки и киберинциденти и своевременно възстановяване до

8-%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%86%D0%B8%D0%B8

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

нормалното състояние.

За да се постигне тази стратегическа цел на национално ниво в Стратегията са предвидени три последователни фази, със завършването на които ще се достигне до различна степен на зрялост.

Фаза 1 (инициираща): Инициране и постигане на базов капацитет за киберсигурност - киберсигурни институции

Фокусът е върху постигането на минимално общо ниво на МИС на ниво отделни организации/нормативно задължени субекти, изграждане на Национална координационно-организационна мрежа за киберсигурност със съответните механизми, процеси и техническа платформа, чрез която се осигурява предаване на информация и се осъществява оперативно сътрудничество. Следва да бъдат проведени кампании за формиране на базово ниво на киберхигиена за уязвими обществени групи, както и да бъде изградена система за изследвания и образование и сертификация на хора и технологии в сферата на киберсигурността.

Фаза 2 (развитие - от капацитет към способности): киберустойчиви институции и “киберсигурно” общество.

Във фокуса на тази фаза е поставена организацията на капацитета за реализиране на устойчивост на ниво отделни организации и способности за координиран отговор при киберинциденти и кризи, систематични дейности по превенция.Институционализиране на устойчив механизъм за взаимодействие при мащабни киберинциденти и кампании, заплахи от кибер и хибридни кризи.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Фаза 3 (зрялост): киберустойчиво общество.Основните дейности по трите фази, очакваните резултати и индикаторите за изпълнение се определят с Пътната карта към Стратегията.

III. 2 Необходимост от създаване на компетентни органи в сферата на киберсигурността според Директива 2016/1148:

Директивата поставя изискване пред държавите-членки да определят повече от един национален компетентен орган, отговарящ за изпълнение на задачите, свързани със сигурността на мрежите и информационните системи на операторите на основни услуги и доставчиците на цифрови услуги.

В изпълнение на това изискване нормативно е предвидено Министерският съвет да определя административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност за секторите и услугите.

С решение № 192 на Министерския съвет4 за определяне на административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност.

Формирането на единна политика за киберсигурност е отговорност на всички държавни органи, но основите и насоките се полагат от Народното събрание, Министерския съвет и Президента на републиката. Функциите и отговорностите по киберсигурността са разпределени между висшите държавни органи както следва:

[4]https://www.mtc.government.bg/sites/default/files/rms192imetodika.pdf

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Народното събрание на Република България осигурява приемането на закони и други актове, свързани с киберсигурността и упражнява парламентарен контрол.

Президентът, в качеството му на Върховен главнокомандващ на въоръжените сили на Република България, получава цялостна информация за състоянието и развитието на Националната система за киберсигурност, а при въвеждане на „извънредно положение“, „военно положение“ или „положение на война“ ръководи дейностите по осигуряване на киберустойчивост на държавното и военното управление.

III. 3 Министерски съвет и Министър на електронното управление – необходимост от връзка с ведомствата в сферата на киберсигурността

Управлението на Националната система за киберсигурност се осъществява от **Министерския съвет** в съответствие с Конституцията, законите и подзаконовите нормативни актове и при съобразяване с целите и приоритетите, посочени в приети стратегически документи.

За реализацията на Стратегията, Министерският съвет приема Пътна карта и следи за постигане на приоритетите и целите, както и за осигуряване на необходимите ресурси за изпълнение на заложените дейности.

Законът за кибересигурност е определил правомощията на **Министъра на електронното управление в сферата на киберсигурността и мрежовата и информационна сигурност.** На него е възложено провеждането на държавната политика в областта на мрежовата и информационната сигурност. Негова е отговорността по изготвяне и предлагане за приемане на Нациална сгратегия за

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

мрежова и информационна сигурност. Сред кръга от правомощия е удостоверяването на съответствието на внедряваните от административните органи информационни системи с изискванията за мрежова и информационна сигурност и упражнява контрол върху администрациите за спазване на тези изисквания. **Министърът на електронното управление е натоварен с упражняването на контрол за спазване на изискванията за МИС на административните органи**. Министърът има право, а и задължение да извършва проверки чрез оправомощени от него лица на информационната сигурност на дадена информационна система или на предприетите от страна на проверявания административен орган мерки, като може да издава предписания, с които да даде насоки за подобряване на мерките.

Сред другите правомощия на Министъра на електронното управление е и разработването на методика и правила за извършване на оценка за съответствие с мерките за МИС.

Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво.

Министерството на електронното управление координира дейностите по изграждане на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център в сътрудничество с Държавна агенция "Национална сигурност", Министерството на вътрешните работи и Министерството на отбраната.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

За координация и обмен на информация при възникване на инцидент или при извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт с цел осведоменост на компетентните по случая институции и изготвянето на общ отговор. Процедурите и правилата за това сътрудничество се определят със споразумение за взаимодействие между заинтересованите ведомства.

За координиране на дейностите за реакция при кибератаки и мащабни инциденти министърът на електронното управление може да създава междуведомствени оперативни групи с участието на ведомства, организации и институции, включително от частния сектор, имащи отношение към тези дейности.

Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност - в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност.

III. 4 Специализирани структури към МС/министъра на електронното управление:

- **Съвет по сигурността към МС**

Съветът по сигурността[5] към Министерския съвет анализира състоянието на системата за защита на националната сигурност, изготвя оценки и предлага решения и действия, по отношение осигуряване и защита на мрежовата и информационната сигурност от посегателства, включително и по отношение на способностите за

[5] https://saveti.government.bg/web/cc_1901/1

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

противодействие на заплахи и управление при киберкризи, като съществен елемент от дейностите по защита на националната сигурност.

Координирането на действията на **политическо и стратегическо ниво** за гарантиране постигането на необходимите капацитет и способности за киберсигурност, се осъществява от постоянно действащ консултативен орган **Съвет по киберсигурност** към Министерски съвет. Съветът осигурява сътрудничеството между компетентните държавни органи, бизнеса, академичния сектор, неправителствените организации при определянето и провеждането на държавната политика в областта на киберсигурността. Съставът и функциите на Съвета се определят със Закона за киберсигурност. Председател на Съвета е заместник-министър председател, определен от министър-председателя. Организацията на дейността на Съвета се урежда с акт на Министерски съвет[6].

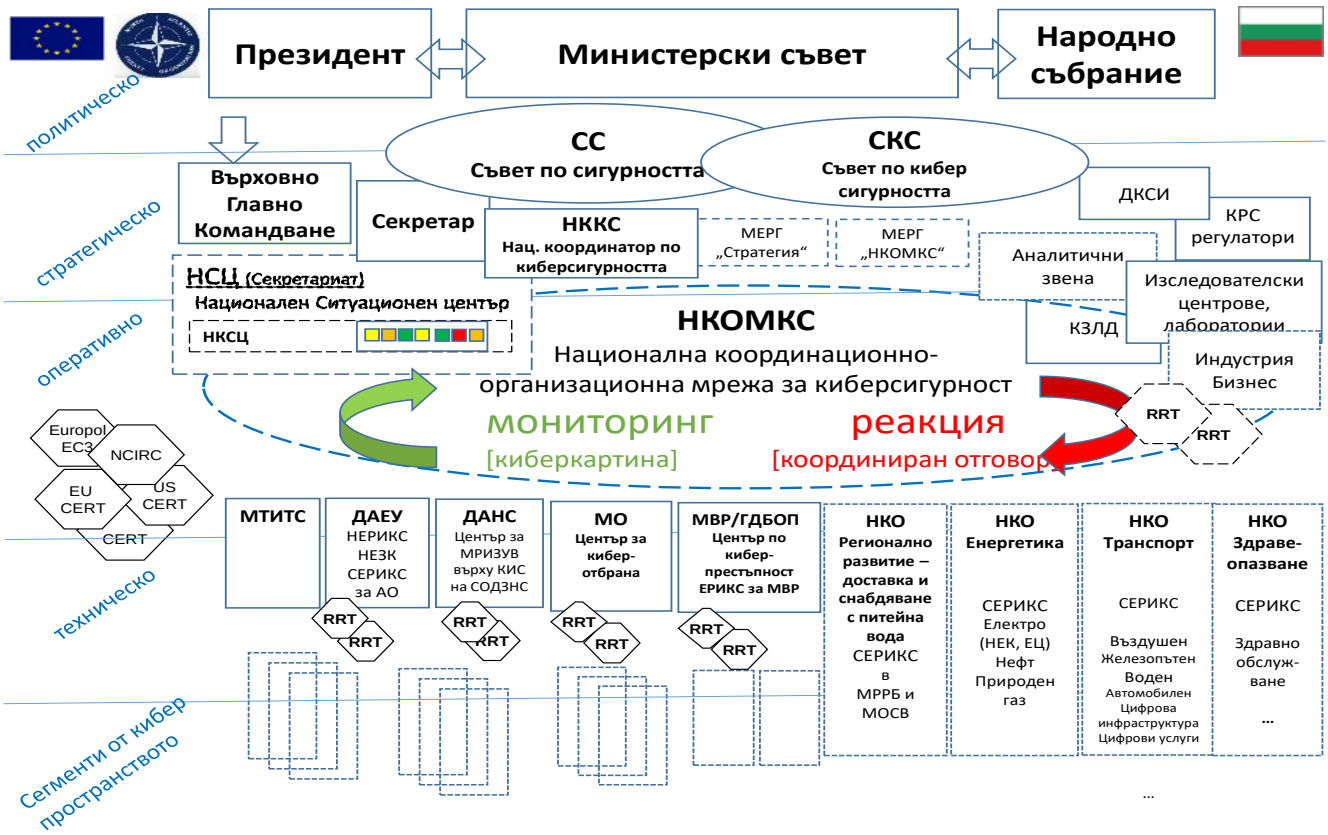
Отговорността за разработване на адекватни секторни политики и/или стратегии за постигане на киберсигурност, планиране и изпълнение на мерки за развитие на съответни способности имат административните органи, принадлежащи към системата на изпълнителната власт, както и всеки друг орган, носител на административни правомощия, овластен въз основа на закон, включително лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, както и публичните и частните субекти и операторите на критични инфраструктури, доставчиците на информационни и обществени електронни съобщителни мрежи и/или

[6] Правилник за организацията и дейността на Съвета по киберсигурност - https://lex.bg/bg/laws/ldoc/2137198634

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

услуги. Всички посочени участници имат пряка отговорност в своя сектор и споделена отговорност и ангажимент за ефективното участие в националните мерки и планове, осигуряването на съответните ресурси за развитие на капацитет и способности за последователно постигане на мрежова и информационна сигурност, киберсигурност на цялото общество, бизнеса и държавата.

✓ ***<u>Общ модел на Националната система за киберсигурност</u>[7]:***



[7] Източник: Актуализирана Национална стратегия „Киберустойчива България 2023”

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Национална координационно-организационна мрежа за киберсигурност** (НКОМКС):

За постигане на определените в Актуализираната Национална стратегия „Киберустойчива България 2023" Цел 2 и Цел 3 и за координация на **оперативно ниво** се създава организационна мрежа - **Национална координационно-организационна мрежа за киберсигурност** (НКОМКС) със съответна техническа платформа**,** както и **Национален киберситуационен център** (НКСЦ) в рамките на Националния ситуационен център със следните основни функции:

➢ **Мониторинг на националната киберкартина** - състояние на киберпространството в държавата, обобщена информация и индикация за статуса и безпроблемното функциониране на комуникационните и информационни системи (включително електронните съобщителни системи, преносните мрежи, националната и международната информационна свързаност). За целта се определя стандартизиран протокол и многостепенен код на състоянията (съгласуван с установените кодове за кризи, както и с тези на ЕС, НАТО и партньорски мрежи), връзка към споделяната техническа информация (на ЕРИКС/CERT[8] също CSIRT/CIRC и др.), анализ на възможните причини и източници, оценка на въздействието, както и ефективност на предприетите мерки и действия. Способност за оценка в реално време и вземане на решения по киберсигурността.

[8] **ЕРИКС** - Екипи за реагиране при инциденти с компютърната сигурност; CERT - Computer Emergency Response Team/Computer Emergency Readiness Team; CSIRT - Computer Security Incident Response Team; CIRC – Computer Incident Response Capability/Center (NATO).

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Координиран отговор** и оперативно взаимодействие при мащабни инциденти, комплексни атаки и кризи – осъществява се с организационно-технически средства и се базира на актуалната киберкартина, анализа на състоянието и чрез технически протокол и организационни мерки се предоставя информация за състоянието на национално ниво, за възможни комбинирани заплахи и хибридни въздействия, за потенциален кинетичен и каскаден ефект и се дават препоръки за превантивни действия на оперативно и тактическо/техническо ниво, за активиране на планове и действия от киберотбраната, привличане на експерти (от работните групи към СКС, международни и др.)

НКОМКС представлява „**нервната система**“ на Националната система за киберсигурност. Включените в НКОМКС организации интерактивно взаимодействат, като непрекъснато изпращат към НКОМКС информация за киберсъстоянието си за целите на националния мониторинг и съответно **получават актуалната киберкартина за страната, оперативна оценка** на общата ситуация, указания и препоръки за координация и взаимодействие с други организации.

Задължение на всеки участник в НКОМКС е да **действа незабавно и автономно** в рамките на своите компетентности, планове и способности. На базата на получаваната обща оценка на ситуацията и на цялостната киберкартина, тези действия се адаптират, разширяват и координират с други центрове и организации. Всички участници предприемат **превантивни действия** и повишат динамично състоянието си на готовност на базата на собствен анализ и оценка, с отчитане на националната киберкартина и препоръките по НКОМКС.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Гръбнакът на НКОМКС се изгражда на базата на структури, центрове и организации, отговорни за киберсигурността в различни сегменти на киберпространството:

- Национален ЕРИКС в рамките на Министерство на електроното управление (МЕУ);
- Национално единно звено за контакт в рамките на МЕУ;
- Секторни ЕРИКС в МЕУ и към Националните компетентни органи, определени с решение на МС;
- Център за киберотбрана (Mil CIRC – Computer Incident Response Capability) в Министерство на отбраната (МО)
- Център по киберпрестъпност в ГДБОП-МВР;
- ЕРИКС в ГДБОП-МВР;
- Център по киберсигурност – Дирекция КИС-МВР;
- Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху КИС на стратегически обекти и дейности от значени за националната сигурност в ДАНС;
- ЕРИКС за класифицирани мрежи в ДАНС;
- Национален център за контратероризъм в ДАНС;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- Аналитични звена;
- Регулаторни и акредитиращи структури;
- Изследователски и други специализирани звена.

- **Национален координатор по киберсигурността**

Министър- председателят на Република България определя национален координатор по киберсигурността, който е и секретар на Съвета по киберсигурност.

Националният координатор по киберсигурност осигурява връзката между двете нива на Системата за киберсигурност - стратегическото ръководство и системата за координация на оперативно ниво, както и връзката с Националната система за управление при кризи. Националният координатор участва при изграждането и развитието на НКОМКС и осигуряването на нейната надеждност, сигурност и устойчивост и в създаването и развитието на НКСЦ, като обособена структура в Националния ситуационен център. В националния ситуационен център е разположен национален център за непрекъснат мониторинг на киберкартината в страната и осигуряване на координирана реакция.

Функциите на Националния координатор по киберсигурност се определят със закон, като в случая това е Законът за киберсигурност. Съгласно посочения нормативен акт Националният координатор по киберсигурността ръководи изготвянето и актуализирането на националната стратегия за киберсигурност и пътната карта към нея.

Сред по- забележимите му функции следва да посочим, че предлага на Съвета по киберсигурността:

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- нива за оценка на заплахата от кибератаки и киберинциденти и критерии за определянето им;

- степени за определяне нивото на готовност за противодействие на кибератаки и киберинциденти - в зависимост от нивото на заплаха;

- мерките, които да се предприемат при съответните степени на готовност;

В допълнение, Националният координатор по киберсигурност осигурява взаимодействие и подпомага дейността на секретаря на Съвета по сигурността към Министерския съвет.

- **Национално единно звено за контакт:**

Към МЕУ е създадено Национално единно звено за контакт[9]. Националното единно звено за контакт координира въпросите, свързани с мрежовата и информационната сигурност, както и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави- членки на ЕС. Националното единно звено за контакт уведомява Европейската комисия за обхвата на задачите на ЕРИКС. Задължение на звеното е да уведоми Европейската комисия за приетата Национална стратегия за МИС.

[9] https://psc.egov.bg/psc-common-info

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

IV. Анализ на съответствието между националното законодателство и Директива 2016/1148

Директива 2016/1148 предвижда минимална хармонизация за своите разпоредби в националните законодателства на държавите- членки на ЕС, но въпреки това България е сред държавите, които са транспонирали Директивата до голяма степен като в националното законодателство намират отражение всички съществени моменти, предвидени с Директивата.

Все пак следва да се има предвид, че Директивата има своето действие от 2018 г като националното ни законодателство също датира от м.ноември 2018 г., като до този момент сферата на киберсигурността и обществените отношения, които биват засегнати в тази връзка не съществува никаква правна регламентация.

За България киберсигурността, киберотбраната, цифровата трансформация на електронното управление са нови аспекти, над които следва да се положат редица усилия за тяхното усъвършенстване и подобряване за в бъдеще, като можем да приемем, че са положени едни здрави основи с транспонирането на разпоредбите на Директива 2016/1148 в националното ни законодателство.

Специално внимание следва да бъде обърнато на електронното управление в Република България, което дълго време беше абсолютно недостъпно за гражданите и бизнеса, като кризата, породена от вируса на COVID-19 наложи бързата цифрива трансформация на този сектор, така че да бъде осигурена максимална достъпност. Следва да бъде посочено, че България постига неоспорим напредък в рамките на кратки срокове, доколкото преминаването към онлайн работа и общуване беше абсолютно непознат начин до преди пандемията от вируса на COVID-19. България предприе

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

редица стъпки в посока дигитализиране на обществения сектор, но тъй като това се случи за много кратко време, тази трансформация не бе напълно безопасна. **Безопасността и защитата на личните данни на гражданите заемат челно място сред целите, които си поставят държавите-членки в своите стратегически документи в областта на киберсигурността, като това е сектор, в който и България полага сериозни усилия**.

В последните години все повече се налага разбирането, че от сигурността на една държава-членка зависи сигурността на всички. ЕС може да осигури мултидисциплинарен и интегриран отговор, като помогне на участниците в областта на сигурността в държавите членки с необходимите им инструменти и информация, като именно това разбиране води до изготвянето на една обща, унифицирана политика в сферата на киберсигурност, която да гарантира интересите на всички в общността.

Унифицирането на законодателствата и на органите гарантира осигуряването на готовност в ключовите за държавата сектори с цел работещо сътрудничество, адекватна, своевременна и бърза реакция в слчуай на кибер инциденти, както и на своевременно сътрудничество на ниво ЕС.

На този етап националното ни законодателство се намира в пълно съответствие с Директива 2016/1148, което осигурява възможност за постигането на общата цел за повишаване на нивото на защита против инциденти, рискове и заплати за МИС в ЕС.

Въпреки постигнатия напредък, нивото на киберсигурност както в България, така и в останалите държави-членки на ЕС остава незадоволително и не може да отговори на постоянните предизвикателства. **Това положение в целия ЕС доведе до приемането на изцяло нова регламентация в сферата на киберсигурносттав –**

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Директива - Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

Една от основните причини, които довеждат до приемането на нова Директива в областта на киберсигурността е, че действащата Директива 2016/1148 не предоставя задоволителна защита на европейските граждани, тъй като не може да отговори на постоянно променящите се обстоятелства. Необходимо е да бъдат предприети конкретни действия, който да приведат законодателството в съответствие с развитието на технологиите, така че последното да бъде адекватно.

Тук е мястото да подчертаем, че сферата на електронното управление и най- вече администрациите в лицето на органите на местно самоуправление работят с огромно количество чувствителни данни, включително и лични, като едно от основните предизвикателства, срещу които се изправя цифровата им трансформация е именно гарантирането на сигурността на тези данни.

Извършената оценка на Европейската комисия (ЕК) показва и че нивото на съвместна ситуационна осведоменост и съвместното кризисно реагиране не е достатъчно добре развито, дори напротив отчетени са доста ниски резултати по тези показатели.

Сред другите слабости на сега действащта Директива са посочени контролът и надзорът по прилагането на Директивата, които не се осъществяват в достатъчна степен и дори по места липсва какъвто и да е надзор и предприемане на каквито и да е санкции при констатирани нарушения. Това е и причината в доклада и оценката си ЕК да дава

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

предложение за приемане на нова директива в областта на МИС, която да включи нови изисквания, така че правилата на ЕС в областта на киберсигурността да могат да отговорят на напредъка в сферата на дигитализацията и развитието на технологичните системи.

Предстоящите законодателни промени в националното законодателство в България ще бъдат предмет на разглеждане по- надолу в настоящото изложение.

V. Цифрова трансформация в сферата на електронното управление:

Дигиталната (цифровата) трансформация е процесът по приемане на цифрова технология от организация за дигитализиране на нецифрови продукти, услуги или операции. Целта на прилагането му е да се увеличи стойността чрез иновации, изобретения, потребителско изживяване или ефективност.

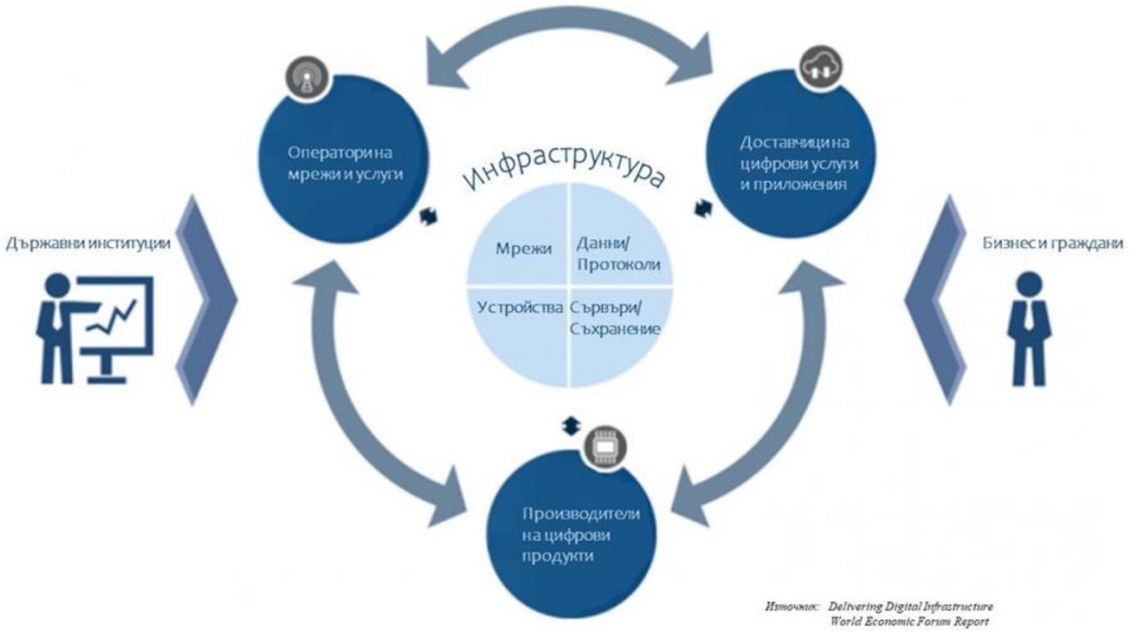
Цифровата трансформация в областта на държавното управление е насочена към превръщането на обработваните и съхранявани данни в основен капитал на обществото. Посредством разработването на оперативно съвместими интерфейси и модели за обработване, съхраняване и предоставяне на достъп до данни се създава възможност за преминаване към отдалечен достъп до редица услуги от страна на гражданите и бизнеса, както и улеснява междуведомствения обмен на данни.

В хода на цифровата трансформация в областта на държавното управление се постига промяна в модела, по който взаимодействат гражданите и бизнеса от една страна с държавата и предоставяните от нея публични услуги, от друга страна. Всички действия имат за резултат намаляване на броя на административните услуги и трансформирането им във

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

вътрешноадминистративни, а основна цел, която си поставя <u>цифровата трансформация в общините</u> е електронната **комуникация между гражданите и бизнеса с администрацията да се превърне в основния и предпочитан метод за това.**

Всичко това ще доведе до значително намаляване и дори премахване на използването на хартия за сметка на електронната форма при издаване на документите. Колкото повече граждани предпочетат комуникацията с администрацията по електронен път, толкова повече се повишава доверието в електронното управление от страна на цялото общество.



www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

За постигане на устойчиво развитие в сферата на елеткронното управление следва да бъде осигурена модерна инфраструктура, която да гарантира възможността за бърз и сигурен обмен на данните. Инфраструктурата следва да може да поддържа увеличаващия се с бързи темпове трафик, както и да осигурява покритие с достатъчен капацитет, гарантиращ успешния обмен на данни.

Според ЕК един от основните инструменти за подобряване на благосъстоянието на обществото във всеки един аспект е широколентовият достъп до Интернет, като всяка държава- членка осигурява недискриминационен, безопасен и ефективен достъп до Интернет. В съвременния свят Интернет заема челна позиция и се превръща в един от решаващите фактори не само в икономически план, но и с оглед социалната адаптация на индивида.

Сред ключовите елементи на цифровата трансформация в България в момента, а **и през следващите няколко години ще бъдат 5G мрежите и оптичните мрежи**. Отделно от това страната ни следва да заложи на сигурността, устойчивостта и надеждността на своята инфраструктура, така че да гарантира сигурността на личните данни на гражданите и бизнеса.

Усилията са концентрирани **в изграждането на ефективна облачна инфраструктура (Държавен хибриден частен облак, ДХЧО), инструменти за обмен на данни, архитектури и механизми за управление на системи за споделяне на данни и изкуствен интелект.**

Централно място в политиката в областта на цифровата трансформация заема осигуряването на достъп до интернет за всички групи потребители, което се явява сериозно предизвикателство в много райони в България, особено в по- малките общини.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

От тази гледна точка е от съществено значение да се съхрани възможността за използване на досегашния механизъм на предоставяне на административните услуги – а именно на място, в съответната община, т.нар. обслужване „на гише“.

Като се вземат предвид реалностите в държавата и високия процент на възрастни хора, които не умеят да работят с компютър и Интернет, както и големият процент на хора без възможност за достъп до такъв, в България на този етап няма изгледи административните услуги да започнат да се предоставят само по електронен път. Въпреки това следва да бъдат предприети действия във връзка с осигуряване на достъп до Интернет до възможно повече групи от населението, както и за повишване на грамотността сред уязвимите групи на обществото.

Киберпространството се характеризира с непознати рискове както за потребителя, така и за администрацията, които изискват повишаване на киберкултурата и киберсигурността на обществото като цяло. Решаващо е да се приложат активни мерки за предпазване от известните видове заплахи и подготовка за неизвестните за постигане на киберустойчивост.

Това включва защитата срещу кибератаки и ефективна и висококачествена киберинфраструктура, както и защитата на неприкосновеността на личния живот и личните данни, като основен компонент на цифровата икономика.

Кибератаките се превръщат в сериозна заплаха в съвременния свят, като непрестанно разширяват своя обхват, като това налага държавата да постави сред приоритетите си на челно място именно киберсигурността и защитата на личните данни на гражданите и бизнеса. Държавата в лицето на МЕУ и органите на местна власт в лицето на общините следва да осигури в максимална степен сигурността във

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

виртуалното пространство на потребителите, както и да осигури адекватна защита на личните данни на гражданите и бизнеса, както и да обезпечи сигурността на самите информационни системи в държавните структури.

С приемането на Закона за киберсигурност е транспонирана в националното законодателство Директива 2016/1148 ЕС, която въвежда мерките за високо общо ниво на сигурност на мрежовите и информационни системи в ЕС.

От съществено значение е **провеждането на сертифициращи обучения в областта на киберсигурността на служителите от държавната администрация** така че да бъде повишена киберкултурата и знанията им относно възможните заплахи, както и запознаването им с механизмите на реакция при евентуална кибератака.

Националната политика за киберсигурност предполага развитие в няколко ключови области: развитие на националната система за киберсигурност и устойчивост; мрежовата и информационна сигурност; засилване на противодействието на киберпрестъпността; киберотбрана и защита на националната сигурност; повишаване на осведомеността, знанията и компетентностите и развитие на стимулираща среда за изследвания и иновации в областта на киберсигурността и международно взаимодействие.

За постигане на киберустойчивост следва да бъде гарантирана и обезпечена сигурността и надеждността на хардуерните и софтуерни устройства, технологиите, информацията, служителите и потребителите, свързаността и оперативната съвместимост на комуникационните канали, системи и услуги.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Електронното управление е неразделна част от цифровата трансформация и е основният фактор, създаващ технологични средства за взаимодействие между гражданите и бизнеса, от една страна, и държавната администрация, от друга.

Сред водещите участици в този процес се открояват общините, които следва да развиват своя капацитет за отворени данни. Данните и превръщането им в основен капитал на обществото са от ключово значение. Необходим е преход от фрагментирани, неструктурирани и нестандартизирани данни към данни, обработвани по предварително разработени оперативно съвместими модели, като за всеки използван за целите на административното обслужване набор от данни има предварително разработен модел на тяхната структура, вписан в регистрите за оперативна съвместимост. По този начин се обезпечава преходът от използвани като основни формати на данни за целите на визуализацията и възприятието им от човек към такива пригодни за взаимодействие между системи.

Политиката на МЕУ въвежда стандартизация на услугите, която предоставя възможност за създаване на множество от свързани данни, като достъпа до тях се осъществява по улеснен механизъм. Ключова е ролята на данните за трансформиране на държавното управление и използване на интелигентни технологични решения за целите на административното управление.

Чрез моделите се определят както правата и задълженията между участниците от различните целеви групи помежду им, така и необходимите за функционирането на моделите съпътстващи технологични и функционални ресурси. Чрез моделите се стандартизират ключови за цифровото управление процеси, като модел за централизирано заявяване, заплащане и предоставяне на услуги, модел за заплащане на задължения, модел за електронна автентикация.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Особено важно е да бъде осигурена възможност за използване на трансгранични електронни услуги, в т.ч. въвеждането на услуги от българските институции, които да могат да се ползват и от граждани на други държави-членки по подразбиране, което на този етап все още не е напълно възможно.

На следващо място, са определени титулярите на определен процес, отговорните за неговото развитие и предоставяне лица. Такива процеси са процесът по автентикация и идентификация, процесът по заявяване и заплащане на задължения, процесът по заявяване на електронна услуга, достъп до данни и удостоверяване по електронен път на вписани в регистри факти и обстоятелства. Моделите и тяхното прилагане изолират участниците от отделните целеви групи до присъщо необходими и предварително определени интерфейси за взаимодействие. Моделите осигуряват предоставянето и изпълнението на определените процеси, независимо от степента на технологична обезпеченост на отделните участници.

Цифровата трансформация на публичния сектор способства за достъпността на трансграничните е-услуги, от които гражданите и предприятията се нуждаят когато пътуват, работят, учат или извършват стопанска дейност в рамките на ЕС.

В съответствие с Регламент (ЕС) 2018/1724 на Европейския парламент и на Съвета от 2 октомври 2018 година за създаване на единна цифрова платформа за предоставяне на достъп до информация, до процедури и до услуги за оказване на помощ и решаване на проблеми и за изменение на Регламент (ЕС) № 1024/2012, до 2023 година държавите-членки на ЕС, следва да осигурят предоставянето на 21 ключови административни процедури изцяло онлайн, като достъп до тези услуги следва да имат както потребителите на място, в техните държави, така и трансграничните потребители.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

VI. Цифрова трансформация на общините в Република България

С изменението на чл. 18а от Административнопроцесуалния кодекс (АПК) се въведе нормативно задължение на административните органи, сред които безспорно са и общините, да осигурят техническа възможност на подателите на сигнали, жалби, протести, молби, искове и приложенията към тях да подадат същите и електронно по реда на ЗЕУ.

ЗЕУ също претърпя редица изменения, които имаха за цел да осигурят ефективни и сигурни електронни услуги на гражданите и бизнеса. Законодателните промени бяха предприети с цел да бъде осигурено разработването, внедряването и надграждането на необходимите ресурси на електронното управление при спазване на изискванията за мрежова и информационна сигурност и оперативна съвместимост.

Чрез измененията и допълненията в ЗЕУ се гарантира на гражданите и организациите като потребители на електронни административни услуги сигурен, надежден и проследим канал за подаване на електронни документи и заявяване, респ. получаване на електронни административни услуги.

На слеващо място легална регламентация получават средствата за електронна идентификация и режима за тяхното признаване. Разпоредбите на нормативните актове са в унисон със Закона за електронната идентификация и Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО;

Въведени се изисквания за системна интеграция при изграждане, поддържане,

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

развитие и наблюдение на работоспособността на информационните и комуникационните системи, използвани от административните органи и се осъществяват от „Информационно обслужване“ АД - първият сертифициран доставчик на удостоверителни услуги в България.

ЗЕУ въвежда административнонаказателни разпоредби, които следва да обезпечат по-строг контрол на прилагането на разпоредбите на закона и по-ефективна превенция на нарушенията. Регламентирани са принудителни административни мерки за предотвратяване и преустановяване на нарушенията по закона и нормативните актове по прилагането му, както и за отстраняване на негативните последици от тях. Регламентирани са нови състави на административни нарушения;

Реализирано е надграждане на „Единен модел за заявяване, заплащане и предоставяне на електронни административни услуги“. Това представлява модел на основния работен процес при заявяване, заплащане и предоставяне на електронни административни услуги (ЕАУ) и реализацията му чрез ресурсите на електронното управление. Основната цел на създаването и реализирането на Единния модел е да се предостави възможност на гражданите и бизнеса за централизирано заявяване, заплащане и предоставяне на електронни административни услуги и информация, свързана с тях.

Целенасоченото и поетапно реализиране на Единен модел за заявяване, заплащане и предоставяне на електронни административни услуги и свързаните с него изисквания към необходимата информационно-технологична инфраструктура е в пълно съответствие с визията на електронното управление в Република България, отнасящи се до:

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- Въвеждане и утвърждаване на ефективни бизнес модели в работата на администрацията за преминаване от рутинни дейности към предоставяне на услуги за гражданите и за бизнеса;

- Изградена цифрова администрация – администрация, структурирана в съответствие със съвременните управленски методи и постиженията на информационните и комуникационните технологии.

- Постигната оперативна съвместимост на национално ниво за преход от фрагментирани и затворени, към интегрирани и технологично независими решения;

- Изграждане на механизъм за координирано планиране и реализиране на всички инициативи за развитие и популяризиране на електронното управление;

- Осигурено предоставяне на административни услуги през единния портал на електронното управление по всяко време, от всяко място и чрез различни устройства.

Принципите, в съответствие с които е разработен Единния модел са:

- Предоставяне на ЕАУ „от начало до край“;

- Еднократно събиране и създаване на данни (Once Only);

- Дигитално по подразбиране (Digital by Default);

- Една точка за достъп до ЕАУ – чрез модела ще се създадат условия, заявяването на електронни услуги и средствата ;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- Еднократна автентикация (Single SignOn);

- Оперативна съвместимост по подразбиране (Interoperability by Default)- Оперативна съвместимост (ОС) и семантична оперативна съвместимост (СОС);

- Защита на личните данни и неприкосновеност на личността и личния живот

- Стандартизация при представяне на данните и на тяхната структура, единни нормативни изисквания и индустриални стандарти към информационните системи и е-услугите;

- Проследимост на трансакциите;

- Трансграничност по подразбиране (Cross-border by Default);

- Процес, управляван от потребителя;

- Проактивност, там, където е възможно;

- Представяне по недискриминационен начин.

Усилията на МЕУ за реализацията на Единния модел в съществена степен допринасят за постигане на:

- Ориентирано към потребителя обслужване чрез активно използване на електронни услуги

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- Наличност и достъпност на е-услугите;
- Адаптиране към бързо-изменящата се бизнес среда;
- Вземане на информирани управленски решения;
- Оптимизиране на цената за доставка на е-услугите.[10]

Установява се, че са положени сериозни усилия за повишаване на общото ниво на мрежовата и информационна сигурност в държавната администрация. В МЕУ се изпълняват функциите на Национално единно звено за контакти, на Национален компетентен орган за административните органи, на Национален компетентен орган по мрежова и информационна сигурност по смисъла на ЗКС. Непрекъснат е процесът по координиране на политиките за мрежова и информационна сигурност, като на сайта на CERT България[11] регулярно се издават методически указания, съвети, препоръки и предупреждения. На сайта са публикувани контактните точки за подаване на сигнали за инциденти в информационната сигурност и са разработени, и утвърдени процедури за действия при управление на инциденти, при управление на уязвимости/артефакти.

CERT България предоставя следните електронни административни услуги:

[10]Източник: https://unifiedmodel.egov.bg/wps/portal/unified-model/unified-model/meaning/meaning/!ut/p/z1/nZLRToMwFIafZpfNKRSBXTbOQNwAjbJBb0yBwqqjbLNu7u3tEmbixUDtVXv6n5MvXw4wyIApfpAN17JTfGPeOXNfwkefWolvz4OUeJjGycJzFg8Exw6sfgaS2dzBlCyTmJLACmcesIF-6vb9-Mqh-Hf9AwE2zL8EBmxbygpyq7yZ2g6xUIVdjhy7mKICWwRxXhDf54TUwj6nS6W3eg35h5K1FFXbVWIzwe9Siwnua6gvtoIrqZrvywiu4WHDNlZngBHhYzNyw-BdYwiePVgdpDhCqrp9a1bg6Y-GQgz3Y9bNWtn76DZqzGSu10iquoPsIsn8ytfdjlHjulNafGrI_iN726Zp2vrkhN7q6I44rDgdvwCb6PhE/dz/d5/L2dBISEvZ0FBIS9nQSEh/?urile=wcm%3Apath%3A%2Funifiedmodel%2Fsite%2Funified-model%2Fmeaning%2Fmeaning

[11]https://www.govcert.bg/BG/Pages/default.aspx

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- 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.

Положени са стабилни основи в областта на МИС като освен Наредбата за минималните изисквания към МИС е разработена и приета Методика и правила за извършване на оценка за съответствие с мерките за МИС.

В отделните административни структури се провеждат обучения на служителите, отговорни за МИС по изискванията на ЗКС, НМИМИС, Методиката и правилата за извършване на оценка за съответствие с мерките за МИС, както и останалите нормативни документи.

Налице е функциониращ Регистър на информационните ресурси, който се поддържа от МЕУ[12].

Основната цел на регистъра е да автоматизира дейностите по извършване на инвентаризация на информационната и комуникационна инфраструктура (ИКИ) на централните, областните и общинските администрации, без тази на сектор

[12]https://dev.egov.bg/PDev/publExtData.jsf?idPubl=342

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

„Правосъдие“, за структуриране на информация и данни.

Нивото на цифровизация на администрацията зависи и от степента на изграждане и развитие на споделени информационни ресурси, както и от набора от услуги, които могат да бъдат достъпени чрез тях.

Споделените информационни ресурси на електронното управление са техническата инфраструктура, единната електронна съобщителна мрежа (ЕЕСМ), информационните центрове и държавния хибриден частен облак (ДХЧО), които се създават и развиват първо от ДАЕУ, а след това от МЕУ. Те се използват споделено от всички държавни институции.

Облачните услуги са основен компонент на споделените ресурси на електронното управление, развиват се на основата на изграждане и обновяване на центрове за данни и се базират на облачни платформи и технологии, основни за изграждането на ДХЧО[13].

Държавният хибриден частен облак е основен елемент на споделените ресурси на електронното управление, през който се конфигурират и поддържат мрежови и административни услуги в облачната среда за публичните администрации, които предоставят електронни услуги за гражданите и бизнеса.

Основната цел в областта на електронното управление е насочен към намаляване

[13]https://e-gov.bg/wps/wcm/connect/e-gov.bg-18083/8cfc6aee-e0d9-43d9-acfd-b873aefa70c7/%D0%90%D1%80%D1%85%D0%B8%D1%82%D0%B5%D0%BA%D1%82%D1%83%D1%80%D0%B0+%D0%BD%D0%B0+%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D1%82%D0%BE+%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5+%D0%B2+%D0%A0%D0%B5%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0+%D0%91%D1%8A%D0%BB%D0%B3%D0%B0%D1%80%D0%B8%D1%8F.pdf?MOD=AJPERES&CVID=mNMd7x5&useDefaultText=0&useDefaultDesc=0

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

на административната тежест за гражданите и организациите чрез създаване на технологична възможност за еднинно заявяване, заплащане и предоставяне на електронни администативни услуги.

Единния модел осигурява както намаляване на административната тежест за гражданите и организациите, така и създава възможност за предоставяне на достъпно комплексно обслужване, при което отделни администрации могат да обменят информация помежду си.

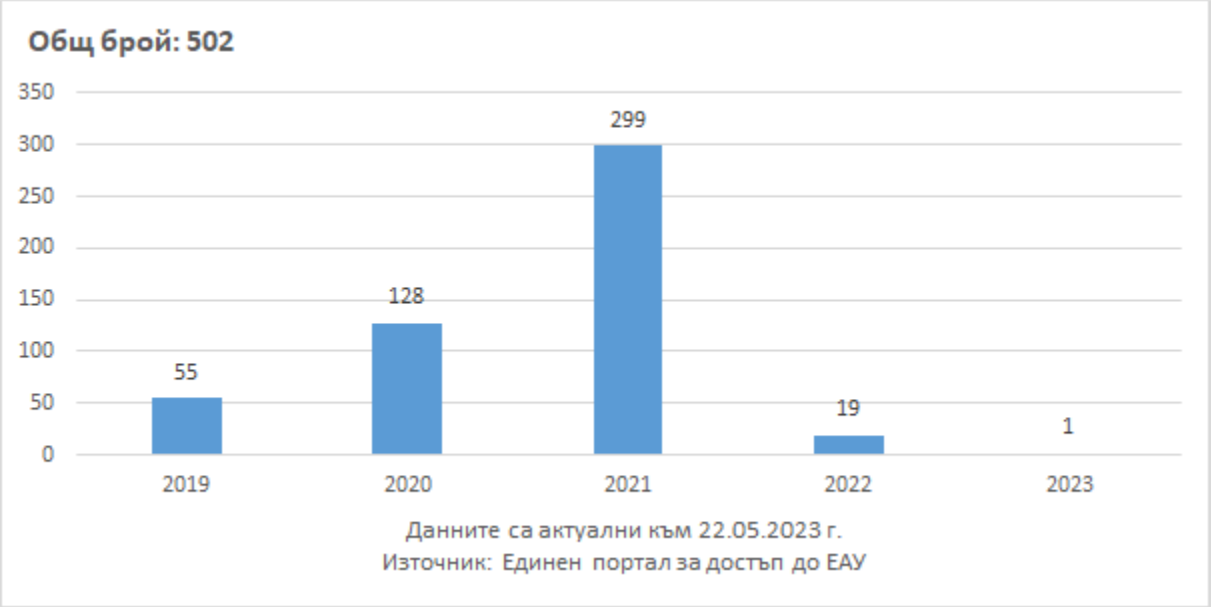
Досега са положени сериозни усилия за развитието и интегрирането на хоризонталните системи на електронното управление, свързани със създаването на Едиинея модел. С увеличаването на потреблението се стимулира развитието на електронни администативни услуги за гражданите и организациите, както и обмена на данни между администрациите.

Хоризонталните системи на електронното управление представляват информационни системи с общи функционалности при предоставянето на каквато и да е административна услуга. Системата за сигурно електроно връчване (ССЕВ) вече се е утвърдила като сигурен и достъпен начин за изпращане, получаване, съхраняване на електронни документи, е-плащания при гарантиране на авторството, интегритета на данните и защитата на личните данни.

Към момента почти всички административни органи са интегрирани към ССЕВ, като регистрираните и активни профили в системата постоянно нараства.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **<u>Присъединени към Единния модел администрации:</u>**

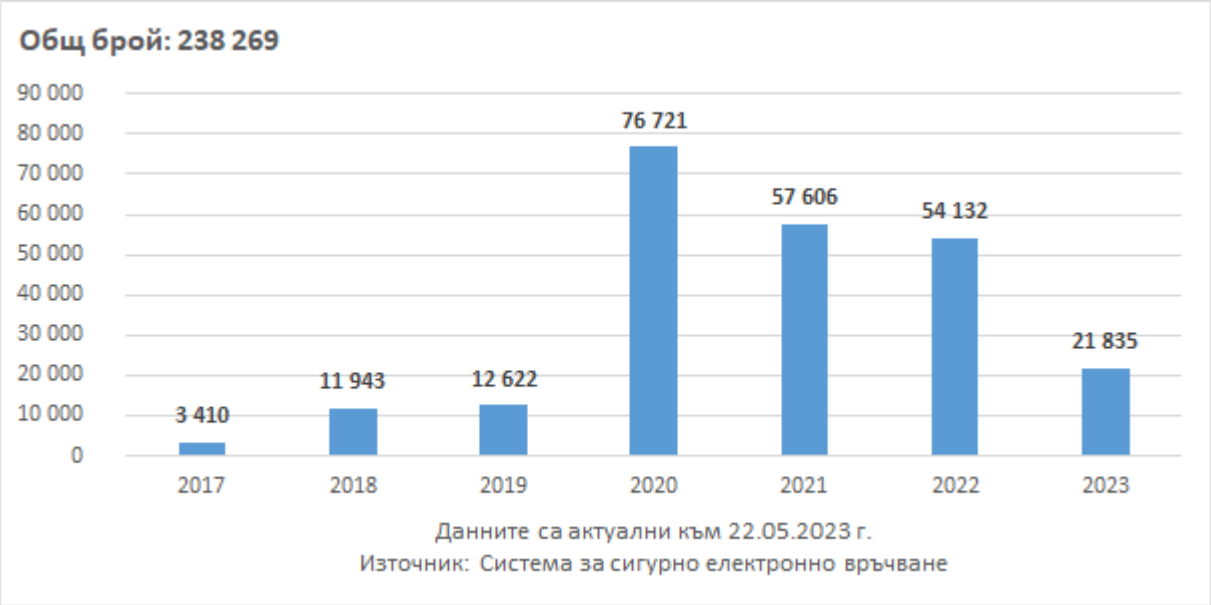


www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **<u>Заявени електронни услуги чрез Единния модел</u>**

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Брой потребители на Система за сигурно електронно връчване (ССЕВ)**



VII. ОБЩИ ИЗИСКВАНИЯ КЪМ ИНФОРМАЦИОННИТЕ СИСТЕМИ И СОФТУЕРНИТЕ КОМПОНЕНТИ

Административните органи, доставчиците на обществени услуги и лицата, осъществяващи публични функции, разработват и публикуват декларация за достъпност по чл. 58в, ал. 4 от ЗЕУ, която има нормативно задължително съдържание, отнасящо се до статуса на съответствие на съдържанието на интернет страницата или мобилното приложение със стандарта, разработен от МЕУ; кои части от съдържанието са недостъпни и поради какви причини, както и наличните алтернативи в случай, че такива са налице.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Институционална идентичност**

Нормативно е поставено изискването интернет страниците на администрациите да отговарят на правилата за институционална идентичност, определени от министъра на електронното управление. Поставени са минимални изисквания спрямо съдържанието, което следва да включва:

- разположението на наименованието и символите на администрацията;
- съдържанието и поредността на елементите в менютата;
- навигационната структура на интернет страниците;
- разполагането на банери с връзки към други интернет страници;
- метаданните за обработване при автоматизирано търсене, както и други метаданни за използване от външни приложения.
- **Софтуерна архитектура:**

На следващо място, нормативно е установено, че всяка функционалност на сървърните компоненти на системите, която е достъпна за потребителите, трябва да е достъпна и като публичен програмен интерфейс чрез уебуслуга. Всички системи трябва да комуникират помежду си единствено с публично документирани програмни интерфейси. Достъпът до програмните интерфейси се определя от ръководителя на съответната администрация.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Когато обхватът на системата предполага използване ѝ от повече от една администрация, то системата следва да бъде изградена по начин, че с една инсталация да могат да бъдат обслужвани всички администрации.

При инсталиране на нова версия системите следва да продължат работа, като единствено в извънредни случаи и единствено поради технологични причини се допуска спиране на работата, но това следва да бъде осъществено извън работно време на администрацията, като за спирането следва да се уведомят Министърът на електронното управление и всички заинтересовани страни най-малко два работни дни предварително.

- **Резервни копия**

Всеки ръководител следва да определи длъжностно лице/лица, което да осигурява автоматизираното създаване на резервни копия на всички данни и електронни документи най-малко веднъж на ден. Задължително резервните копия следва да се съхраняват отделно от данните или електронните документи с оглед осигуряване на тяхната сигурност при евентуална кибератака или в случай на пробив обезпечаване на възможността за тяхното възстановяване.

Резервните копия се криптират с публичния ключ на съответнат администрация, като следва да минават най- малко веднъж в месеца тест за консистентност и интегритет.

- **Дългосрочно съхранение на електронни документи**

На дългосрочно съхранение подлежат електронни документи, по-стари от две години, чийто срок на валидност е изтекъл, освен ако в закон не е предвидено друго.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Относно дългосрочното съхранение на електронни документи, Министърът на електронното управление изготвя насоки

- **Отворен код, документация и авторски права**

Предвижда се системите по чл. 58а, т. 1 ЗЕУ да се разработват с отворен код от началото на всеки проект за изграждане или надграждане.

Нормативно установено е под какви лицензи следва да бъде предоставен публично изходният код и документацията на системите, като това следва да бъде под един от следните:

1. EUPL (European Union Public License);

2. GPL (General Public License) 3.0;

3. LGPL (Lesser General Public License);

4. AGPL (Affero General Public License);

5. Apache License 2.0;

6. New BSD license;

7. MIT License;

8. Mozilla Public License 2.0.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Информационна сигурност**

Всички доставчици на електронни административни услуги са длъжни да използват удостоверения за автентичност на уебсайтове, на които са разположени официалните интернет страници или на които са разположени информационните системи, чрез които се предоставят електронни административни услуги[14].

За обезпечаването на сигурен достъп до интернет страниците и другите услуги в интернет посредством наименование на домейн е поставено изискване да се използва услугата DNSSec (Domain Name Service - Security - Сигурна услуга за името на домейна).

- **Отчитане на астрономическо време**

Информационните системи отчитат астрономическото време по стандарт UTC (Coordinated Universal Time), като когато времето има правно и/или техническо значение се отчита до година, дата, час, минута и секунда. Времето се отчита по националната часова зона (UTC+2).

За синхронизация на часовниците на мрежовите сървъри, използвани от доставчиците на електронни административни услуги, трябва да се използва протоколът NTP V4 (Network Time Protocol, версия 4.0 и сл.), като се осигурява хронометрична детерминация с времевата скала на UTC, или аналогичен.

[14] Чл. 45 от НАРЕДБА ЗА ОБЩИТЕ ИЗИСКВАНИЯ КЪМ ИНФОРМАЦИОННИТЕ СИСТЕМИ, РЕГИСТРИТЕ И ЕЛЕКТРОННИТЕ АДМИНИСТРАТИВНИ УСЛУГИ

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Наименования на домейни**

Наименованията на домейните и поддомейните, използвани от административните органи, се определят от съответния ръководител. Налице е нормативно определени изисквания към начина на наименоване на домейните, както и по какъв начин следва да бъде формиран този домейн, а именно чрез префикса "www" ("World Wide Web"), така и без него.

Официалните домейни, използвани от административните органи, трябва да са в националните домейни от първо ниво - ".bg" на латиница и ".бг" на кирилица, или да са поддомейни на "government.bg".

Официалните домейни, използвани от областните администрации, трябва да са поддомейни на "government.bg". Официалните домейни, използвани от областните администрации, трябва да се формират от транслитерацията на наименованието на съответния областен град; наименованията на домейните на Софийска област са "www.sofia-oblast.government.bg" и "www.sofia-region.government.bg".

Официалните домейни, използвани от общинските администрации, трябва да се формират от транслитерацията на наименованието на съответната община, както и с изписването им на кирилица.

Интернет страниците на общинските съвети трябва да са достъпни от интернет страниците на съответните общински администрации, ако се поддържат отделно. В този случай наименованията на домейните се формират с използване на префикс метод по следния начин: "www.savet.sofia.bg", "savet.sofia.bg" и "съвет.София.бг", съответно.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Мерки за мрежова и информационна сигурност**

По своя характер мерките за МИС са организационни, технологични и технически и се прилагат в съответствие със спецификата на дейността на субекта и трябва да са подходящи и пропорционални на рисковете за постигането на основните цели на мрежовата и информационната сигурност.

Мерките са призовани да гарантират основните цели на мрежовата и информационната сигурност, а именно запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия ѝ жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи на субекта.

Мерките следва да бъдат **разнородни,** с огед осигуряване на многопластова защита, или т.нар. „дълбока отбрана“. Мерките следва да бъдат **конкретни и лесни за възприемане**, за да се обезпечи надлежното им приложение. Мерките трябва да бъдат **ефикасни**, за да могат да постигнат широко въздействие по отношение на потенциалнте заплахи чрез минимално разходване на средства и ресурси. На следващо място мерките следва да бъдат **пропорционални на рисковете** така че да бъде осигурено отпимално съотношение между разходи и ползи. Мерките трябва да бъдат също така **проверими**, за да може субектът да предостави в определени случаи доказателства за ефективното приложение на мерките в съответствие с нормативните изисквния заложени в ЗКС.

VII. Задължения на административния орган в сферата на МИС:

Административният орган, съответно ръководителят на субекта е пряко отговорен за мрежовата и информационната сигурност, дори и в случаите, когато дейността е възложена за изпълнение на трети страни. Административният орган, съответно

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ръководителя на субекта следва да осигури условия за прилагане на комплексна система от мерки за управление на тази сигурност по смисъла на международен стандарт БДС ISO/IEC 2700, което включва всички аспекти на сигурност, включително и физическта.

Административният орган, съответно ръководителят на субекта осигурява нужните ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност.

Административният орган, съответно ръководителят на субекта организира одити за установяване на съответствието на предприетите мерки с изискванията на нормативните актове и приетите стандарти; провежда поне един път в годината периодичен преглед на МИС.

Административният орган, съответно ръководителят на субекта е отговорен за определянето, документирането и разпределянето на отговорности по изпълнението, контрола и информираността относно процесите и дейностите по развитие, поддръжка и експлоатация на информационните и комуникационни системи. Тук основополагащ принцип е, че едно лице не може да контролира собствената си дейност, с оглед на което се осигурява контролът на друго лице.

- **Задължение за разработване на политика за сигурност:**

Всеки административен орган или субект следва да разработи и приеме собствена политика за мрежова и информационна сигурност, която следва да бъде преразглеждана ппне веднъж в годината.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Политиката съдържа разписани стратегическите цели на конкретния субект за мрежова и информационна сигурност, както и подхода за тяхното постигане, което следва да бъде в съответствие с общите стратегически и оперативни цели на субекта, нормативните актове и националните стратегически документи в областта.

В политиката следва да намерят отражение всички специфични елементи на сигурност на информационните и комуникационни системи като: обмен на информация, използване на мобилни устройства, работа от разстояние, използване на криптографски механизми, управление на достъпите и автентикацията, разработване на нови системи, управление на инциденти, взаимоотношение с трети страни, повишаване на квалификацията на служителите и на осведомеността по отношение на мрежовата и информационната сигурност и др.

- **Задължение за поддържане на документация:**

Субектът следва да поддържа следната документация:

1. опис на информационните активи;

2. физическа схема на свързаност;

3. логическа схема на информационните потоци;

4. документация на структурната кабелна система;

5. техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;

6. инструкции/вътрешни правила за всяка дейност, свързана с администрирането,

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

експлоатацията и поддръжката на хардуер и софтуер;

7. вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.

Поддържането и съхраняването на тази документация се налага с оглед намаляване на времето за реакция при инцидент, намаляване на загубите, вследствие на реализиран инцидент, както и с оглед намаляване вероятността от възникване на инциденти.

Посочената по- горе документация следва да бъде еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др. Тя следва да се поддържа в актуално състояние, като се преразглежда и в случай на нужда се актуализира. Преразглеждането и актуализацията следва да се осъществяват поне веднъж в годината. Документацията като вид и обем се одобрява от административния орган, респ. ръководителя на субекта или от упълномощено от него лице. Документацията е класифицирана по клас и вид, като е достъпна само за тези лица, които е необходимо да я използват в рамките на служебните си правомощия.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Задължение за поддържане на информация относно изпълнението на изискванията на МИС:**

Административният орган, съответно ръководителят на субекта е задължен да поддържа информация, установяваща надлежното изпълнение на изискванията за МИС, формулирани в нормативните актове.

Информацията следва да бъде актуална и достъпна, като достъп до нея имат само тези лица, на които е необходимо да я използват във връзка с изпълнение на служебните си задължения или са представители на съответните национални компетентни органи, или други оправомощени организации.

- **Класификация на информацията:**

Административният орган, съответно ръководителят на субекта следва да разпише и приеме вътрешни правила за класификация на информацията, които следва да дадат информация как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага органът или субекта. Препоръчителната класификация е посочена в Приложение № 2 към чл. 6, ал. 1 и 7 от Наредбата за минималните изисквания за МИС.

Приемането на вътрешни правила за класификация на информацията осигуряват достатъчна, адекватна и пропорционална защита на информацията с оглед на нейната важност и чувствителност.

Следва да се отбележи, че за класификацията на документацията във връзка с МИС е недопустимо използването на нивата на класификация за сигурност на

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

информацията от обхвата на Закона за защита на класифицираната информация, както и техния глиф!

- **Управление на риска:**

Административният орган, съответно ръководителят на субекта осъществява анализ и оценка на риска за МИС поне веднъж годишно, а в случай на нужда от изменение на условията на работа, информационната и комуникационната инфраструктура, дейностите или процесите в областта на МИС и по- често.

Анализът и оценката на риска предствлява документиран процес, в който се описват нивата на неприемливия риск и отговорността на участниците в отделните етапи на процеса.

Анализът и оценката се извършват по методика, разработена и одобрена от административния орган, съответно ръководителя на субекта. Методиката се свежда до знанието на лицата, които взимат участие в процеса по анализ и оценка на риска. В приложение № 3 към Наредбата е разписана примерна методика.

Административният орган, съответно ръководителят на субекта изготвя план за намаляване на неприемливите рискове като резултат от осъществения анализ и оценка на риска, като планът следва минимално да включва следните мерки:

1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;

2. необходими ресурси за изпълнение на тези мерки;

3. срок за прилагане на мерките;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

4. отговорни лица.

- **Управление на информационните активи:**

Административният орган, съответно ръководителят на субекта разработва и приема свои вътрешни правила относно процеса на управление на жизнения цикъл на информационните и комуникационните системи и техните елементи.

Вътрешните правила трябва еднозначно да указват условията, начина и реда за придобиване, въвеждане в експлоатация, поддръжка, преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти.

Информационните активи съдържат информация за разрешаването на инциденти, анализ и оценка на риска, управление на уязвимости и управление на измененията, като:

1. еднозначна идентификация, като инвентарен, сериен номер или др.;

2. основни характеристики;

3. услуги, процеси и дейности, в които участва;

4. местоположение;

5. година на производство, където е приложимо;

6. дата на въвеждане в експлоатация, където е приложимо;

7. версия, където е приложимо;

8. местонахождение на свързаната с него документация (техническа,

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

експлоатационна, потребителска и др.);

9. отговорно лице.

- **Сигурност на човешките ресурси.**

Административният орган, съответно ръководителят на субекта следва да предприеме целенасочени стъпки по ограничаване и намаляване на риска от инциденти, настъпили вследствие на целенасочена или случайна дейност на свои служители. Гаранция за това са разработени и приети от органа или ръководителя на субекта вътрешни правила и инструкции, чиито адресати са служителите, имащи отношение към процесите и дейностите в обхвата на МИС. Административеният орган съответно ръководителят на субекта следва да осигурят и гарантират, че служителите ще имат подходяща квалификация, знания, умения и опит за изпълнение на своите отговорности, както и да се грижи за периодичното повишаване на квалификацията и експертизата на своите служители.

С вътрешните правила се регламентират условията и процедурата за заемане на длъжност в съответствие със съответните закони и подзаконови нормативни актове, правилата за професионална етика и класификацията на информацията, до която имат достъп служителите и предполагаемите рискове.

На следващо място, с вътрешните правила се регламентират задълженията и отговорностите на служителите по отношение на сигурността на информацията при прекратяване или промяна на правоотношенията им.

Вътрешните правила следва да регламентират и процедурата по ангажиране на дисциплинарната отговорност на ангажираните в сферата на МИС служители при

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

установяване на виновно нарушение на политиката и вътрешните правила за мрежова и информационна сигурност.

Административният орган, съответно ръководителят на субекта гарантира и обезпечава нивото на мрежова и информационна сигурност чрез подходящо професионално обучение за повишаване на квалификацията на служителите; провежда периодично инструктиране на служителите за запознаване на служителите за новите аспекти на МИС, както и с цел повишаване на вниманието им. За проведените инструктажи следва да се води документация, която да позволява да бъде проследено във времето кои служите и кога са били инструктирани.

- **Управление на взаимодействията с трети страни**

При установяване на взаимоотношения с трети лица, административният орган, съответно ръководителят на субекта следва да разпише договорни изисквания за МИС, в това число и относно сигурност на информацията, свързана с достъпа на представители на трети страни до информация и активи на органа/ субекта.

Следва да бъдат разписани ясни договори, по силата на които третото лице следва да поеме задължение също да прилага адекватни мерки за мрежова и информационна сигурност, включително да бъдат включени клаузи за доказването на прилагането на тези мерки чрез документо и/или чрез проведане на одити.

В договорните отношения с трети лица следва да бъде обезпечен произходът на предлаганите активи/услуги и тяхната собствена сигурност, така че органът или субектът да не бъде изложен на неоправдан риск.

За гарантиране на добросъвестност у контрагентите задължително следва да

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

бъдат предвидени негативни последици за третото лице при неспазване на изискванията на органа/субекта за сигурност на информацията, както и отговорност при неизпълнение в срок, количество и/или качество, което би изложило на риск мрежовата и информационната сигурност на органа/субекта.

В договорите следва да бъде разписана процедура за взаимодействие в случай на възникване на инцидент с посочване на котактни точки, начин и ред за подаване на сигнал, време за реакция и възстановяване на работата, условия за приключване (затваряне) на инцидента.

- **Управление на измененията в информационните активи**

Административният орган, съответно ръководителят на субекта следва да разпише и приеме вътрешни правила за управление на измененията в съществените за дейността му информационни активи, което има за основна цел редуциране на риска от инциденти, настъпили вследствие на изменения в информационните и комуникационните системи и обслужващата ги инфраструктура, както и в процесите и дейностите, в конфигурациите, в софтуера или във фърмуера.

Преди да предприеме каквото и да е изменение органът/субектът има задължението да изготви анализ и оценка на риска, а също и да осъщетсви планиране на изменението, така че то да се случи в конкретно предварително определени срокове.

Измененията следва да бъдат предварително съгласувани с всички страни и участници, имащи отношение към процесите и дейностите, свързани с мрежовата и информационната сигурност. Преди да бъдат интегриани, измененията следва да бъдат проверени в тестова среда.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Всяко изменение подлежи на одобрение от административния орган, съответно ръководителя на субекта или на упълномощено от тях лице, както и следва да бъдат оповестени поне три дни преди извършване на изменението по подохдящ начин на всички заинтересовани.

- **Сигурност при разработване и придобиване на информационни и комуникационни системи**

При разработване на проекти и технически задания административният орган, съответно ръководителят на субекта следва да заложи адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е предвидено още в етапа на разработка и внедряване.

VIII. Защита

- **Сегрегация**

Административният орган, съответно ръководителят на субекта поддържа информационна и коникационна информация, с оглед установяване, че информационните и комуникационните системи, изпълняващи различни функции, са разделени и изолирани помежду си физически и/или логически, както и че са разделени и изолирани от информационните и комуникационните системи на трети страни, с цел да се ограничи разпространението на инциденти с мрежовата и информационната сигурност. Когато дадена система е съставена от подсистема, те следва да бъдат разделени по начин, че физически и логически да не съществуа връзка помежду им.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Филтриране на трафика**

Административният орган, съответно ръководителят на субекта следва да гарантира контролиран трафик между отделните систем и подсистеми чрез подходящо филтриране (по IP адрес, по протокол, по номер на порт от Transmission Control Protocol (TCP)/Internet Protocol (IP) стека и т. н.). Това разделение се налага с оглед осъществяване на превенция на атаки и ограничаването на инциденти.

Филтрирането на трафика следва да се осъществява по строго разписани и утвърдени правила от страна на органа/субекта. Правилата подлежат на периодична проверка, актуализация и изменение.

- **Неоторизирано използване на устройства:**

Административният орган, съответно ръководителят на субекта следва да разпише и приеме ясни политики относно използването на лични технически средства в мрежата, която контролират и на преносими записващи устройства.

Тези политики намират своето отражение във вътрешните правила на органа/субекта, като тяхното приемане е обосновано от заплахата за мрежовата и информационна сигурност от използването на тези устройства

- **Криптография**

Административният орган, съответно ръководителят на субекта разработва и приема политика и вътрешни правила за прилагане на криптографски механизми, чиято цел е да гарантират на конфиденциалността и интегритета на чувствителната информация и личните данни в съответствие със съответната класификация на тази информация.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Криптографските механизми зависят от характера и степента на уязвимост на данните към заплахи за нейните конфиденциалност и интегритет.

- **Администриране на информационните и комуникационните системи**

Административният орган, съответно ръководителят на субекта следва да осигури прилагането на мерки за защита на профилите с администраторски права за информационните и комуникационните системи и техните компоненти. Нормативно са усановени изисквания към администраторските профили, като същите са персонални и се използват само и единствено с административни цели. Правата на всеки отделен администраторски профил са ограничени единствено до функционалния и технически периметър на всеки отделен администратор.

Административният орган, съответно ръководителят на субекта поддържа списък на администраторските профили за информационните и комуникационните системи и техните компоненти, като паролите за достъп до администраторските профили се променят периодично, най- малко веднъж в годината, както и при прекатяване на правоотношението със съответния администратор. Паролата подлежи на задължителна промяна при доказан пробив в мрежовата и информационната сигурност.

Всички предприети от администраторите действия подлежат на запис и документиране, като това важи за всеки администраторски профил, поотделно.

- **Среда за администриране**

Административният орган, съответно ръководителят на субекта следва да използва отделна и подходящо защита среда за целите на администриране на

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

информациите и комуникационните системи и техните компоненти. Тази мрежа, система или софтуер следва да бъде изолиана от останалите информационни и комуникационни системи на органа/субекта и от Интернет и да не се използва за никакви други цели.

- **Управление на достъпите**

Административният орган, съответно ръководителят на субекта има нормативноустановеното задължение да предоставя достъп до информационните и комуникационните си системи на потребител или автоматизиран процес само, когато този достъп е нужен на потребителя, за да изпълни задълженията си, или на процеса е нужно да осъществи съответните технически операции.

Административният орган, съответно ръководителят на субекта следва да гарантира, че достъп до информационните и комуникационните му системи имат само оторизирани потребители, устройства (включително други информационни системи) и автоматизирани процеси. Във връзка с изпълнение на това задължение, органът/субектът следва да предвиди в своите вътрешни правила услоция за предоставяне на право на достъп до конкретни информационни активи на служителите с оглед тяхната длъжност и реда за заявяване, промяна и прекратяване на достъпа.

Административният орган, съответно ръководителят на субекта е длъжен да прилага задлъжителни мерки за автентикация, оторизаия и одит на компютърните мрежи и системи, като в тази връзка се поставят определени изисквания към символите в посочените пароли за достъп (наличие на голяма/малка буква, цифра или символ, изискване за определена дължина).

Административният орган, съответно ръководителят на субекта следва да

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ограничи даването на привилегирован достъп, като когато е предоставен той следва да бъде осъществяван под завишен контрол и само за определен период от време.

- **Защита при отдалечен достъп/работа от разстояние**

При необходимост от отдалечен достъп, административният орган, съответно ръководителят на субекта следва да гарантират, че се използва най- малко двуфакторна автентикация; че се използват само канали с висока степен на защита като Virtual Private Network (VPN). Органът гарантира, че не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

- **Защита на хардуерни устройства**

За намаляване на риска от инциденти, предизвикани от технически повреди, административният орган, съответно ръководителят на субекта осигурява климатико-механичните условия, указани от производителя; осъществява наблюдение на параметрите на тези условия, както и провежда планирана регулярна техническа профилактика на устройствата в съответствие с политиката му за жизнения им цикъл.

С оглед намаляване на риска от неоторизиран достъп, административният орган, съответно ръководителят на субекта има нормативноустановено задължение да разполага устройствата в зони, които са физически и логически защитени в съответствие с класификацията на информацията, с която работят.

- **Защита на софтуер и фърмуер**

Административният орган, съответно ръководителят на субекта следва да инсталира и поддържа само версии на използвания в системите му софтуер и фъруер, които се поддържат от доставчиците или производителите им, както и същите следва да

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

бъдат актуални. Съобразно това административният орган, съответно ръководителят на субекта одобрява софтуера, който ще се използва в неговите информационни и комуникационни системи.

Административният орган, съответно ръководителят на субекта задължително следва да предприеме такива мерки, че да не допусне инсталирането и използването на неодобрен софтуер и фърмъер. Административният орган, съответно ръководителят на субекта следва да предприеме мерки по осъществяването на контрол над използвания софтуер и фъруер, както и да следи за неговата актуалност.

Административният орган, съответно ръководителят на субекта разписва и приема вътрешни правила и инструкции за регламентиране на действията, имащи отношение към поддръжката на библиотеката на използвания софтуер и фъруер в актуално състояние; управлението и достъпа до тази библиотека; своевременното следене и установяване на нови уязвимости в сигурността на използвания в системите софтуер и фъруер, както и проследяване за нови версиим ъпдейти и пачове. Правилата и инструкциите очертават мерките за придобиване и проверка на произхода и цялостта на актуализациите преди тяхното прилагане чрез инсталация.

Административният орган, съответно ръководителят на субекта следва да обезпечи и гарантира, че устройствата и системите са конфигурирани в съответствие с препоръките за сигурност на съответния им доставчик или производител.

Административният орган, съответно ръководителят на субекта съхранява оффлайн (off-line) копие от актуалните конфигурационни файлове и/или описание на настройките, като достъпът до тях не е свободен, а контролиран. Копията подлежат на регулярни тестове за качество и годност.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Защита от зловреден софтуер**

Административният орган, съответно ръководителят на субекта следва да приложи подходящи мерки за защита от проникване и мерки за откриване и справяне със зловреден софтуер в своите информационни и комуникационни системи.

Мерките за защита от зловреден софтуер следва да бъдат приложени спрямо всички компоненти на информационните и комуникационните системи. Мерките следва да бъдат актуални, за да бъдат адекватни и съответни на евентуалните заплахи. Мерките следва да бъдат от естество да осигурят извършване на пълна проверка за наличие на зловреден софтуер поне един път в седмицата; както и да позволяват извършването на проверка на електронната поща и файлове, свалени от Интернет, както и от преносими записващи устройства преди същите да бъдат отворени.

Мерките за защита от зловреден софтуер подлежат на периодичен анализ и оценка, с оглед на подобряване на защитата, когато това е възможно.

- **Защита на уеб сървъри**

Административният орган, съответно ръководителят на субекта следва да осигури защита на уеб сървърите, като предприеме действия по инсталиране на сертификат, издаден от доверена система за сертифициране. Следва да се има предвид че спрямо сертификата има нормативно посочени изисквания, на които последният следва да отговори, за да гаранрира защитата в максимална степен.

С оглед осигуряване на защитата и интегритета на информацията, обменяна с потребителите, уеб сайтът трябва да е достъпен само по протокол Hypertext Transfer

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Protocol Secure (HTTPS), като се използват само криптографски транспортни протоколи в посочени версии.

На трето място с цел осигуряване на защитата на уеб сървърите, органът/субектът следва да предприеме действия по криптиране на информацията, обемняна между сървъра и неговите потребители.

Като следваща мярка, органът/субектът следва да приложи подходящ Web Application Firewall (WAP), който наблюдава и филтрира трафика от и към съответното приложение с цел защита на уеб приложенията от кибератаки.

Друга мярка за защита е да не бъде възможно потребителят да вмъква и поставя данни на места, различни от определените от органа/субекта.

Отново с оглед осигуряване на защитата на уеб сървърите следва да бъдат предприети съответни мерки, които да кодират всички данни, изпращани от потребителя и показвани в уеб страницата с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript.

Органът/ субектът предприема мерки за защита от атаки от типа отказ от услуги (DoS), като налага ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по Url; да се конфигурира типът и размерът на headers, които уеб сървърът ще приеме; да се ограничат времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка, за да се минимизира въздействието и на slow HTTP атаки.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

За защита от brute force атаки да се въведе ограничение на броя неуспешни опити за влизане в системата, след което следва заключване/блокиране на профила. На следващо място, бисквитките (cookies) трябва да имат: флаг за защита (security flag) - този флаг инструктира браузъра, че "бисквитката" може да бъде достъпна само чрез защитени SSL канали; флаг HTTP only - инструктира браузъра, че "бисквитката" може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента;

В главната директория на уеб сайта (website) да се сложи файл robot.txt, който дава указания на уеб роботите (ботове/паяци) колко често да обхождат сайта, както и кои части от него да обхождат и да индексират; ако този файл не съществува, уеб роботите обхождат целия сайт - всяка една негова страница, подстраница, статия, линк и т.н., което крие риск за конфиденциалността на информацията;

- **Защита на Domain Name System (DNS)**

Административният орган/ субектът нормативно има разписани следните следните мерки за защита на DNS, които следва да предприеме:

1. при използване на повече от един DNS сървър, всеки от тях да е разположен в различна мрежа/подмрежа;

2. да прилага DNSSEC (Domain Name System Security Extensions);

3. да минимизира DNS заявките съгласно RFC 7816 на IETF от 2016 г.;

4. да забрани zone-transfers - злонамерени лица могат бързо да определят всички хостове в определена зона чрез трансфери на DNS зони, да събират информация за домейна, да избират цели за атаки, да откриват неизползвани IP адреси и да заобикалят мрежовия контрол на достъпа, за да крадат информация;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

5. в конфигурационния файл да сложи:

а) dmarc (Domain-based Message Authentication, Reporting and Conformance) запис;

б) SPF (Sender Policy Framework) запис.

- **Физическа сигурност**

Административният орган, съответно ръководителят на субекта следва да осигури и физическата защита на информационните си активи чрез приалгане на адекватни и съответни мерки срещу заплахи от неоторизиран физически достъп до тях. Мерките трябва да гарантират наличността, интегритета и конфиденциалността на информационните активи.

Административният орган, съответно ръководителят на субекта следва да осигури защита от пожар, наводнение, химическа и физическа промяна на въздуха чрез предприемане на подходящи и съразмерни мерки, а за осъществяване на непосредствен контрол по физическата защита осъществява и съответно наблюдение.

- **Защита на индустриални системи за контрол**

Когато административният орган, съответно ръководителят на субекта използва индустриални системи за контрол, от функционирането и сигурността на които зависят съществените услуги, които предоставя, той е задължен да приложи подходящи мерки за тяхната защита в съответствие с изискванията на наредбата, ако такива са приложими.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- **Наблюдение**

Административният орган, съответно ръководителят на субекта следва да използва система за автоматично откриване на събития, които могат да повлияят на МИС на важнтие за дейността му системи чрез анализ на информационни потоци, протоколи и файлове, преминаващи през ключови устройства, позиционирани така, че да могат да анализират всички потоци, обменяни между собствените им информационни и комуникационни системи, както и с информационните и комуникационните системи на трети страни.

Наблюдението се организира и провежда съобразно вътрешни правила и инструкции, разработени и приети от органа/субекта.

- **Системни записи (logs)**

Относно системните записи, административният орган, съответно ръководителят на субекта дава следните гаранции, а именно, че:

1. в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори **се регистрират автоматично всички събития, които са свързани най-малко с** автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;

2. в записите за всяко от тези събития **е отбелязано астрономическото време, когато е настъпило събитието;**

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

3. всички компоненти на системите поддържат единно време в съответствие с изискванията на: а) стандарти БДС ISO 8601-1 "Дата и време; б) за синхронизация на часовниците на компоненти на информационните и комуникационните системи трябва да се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;

4. достъпът до информацията е ограничен само до лица, имащи задължения за наблюдението по смисъла на чл. 30, за разрешаването на инциденти с мрежовата и информационната сигурност, за разкриването и разследването на тежки престъпления и престъпления по чл. 319а - 319е от Наказателния кодекс в съответствие с чл. 14, ал. 4, т. 2 и чл. 15, ал. 3, т. 3 от Закона за киберсигурност; достъпът до тази информация трябва да е само за четене;

5. информацията се архивира и се съхранява за период не по-малък от дванадесет месеца при спазване на съответните нормативни изисквания;

6. Субектът трябва да е в състояние да извършва корелация на информацията от различните източници и да правят анализ, за да открият събития, които засягат мрежовата и информационната сигурност.

- **Управление на инциденти с мрежовата и информационната сигурност**

Административният орган, съответно ръководителят на субекта следва да регламентира във вътрешните си правила всички дейности по обработката на сигнали и реакция при инциденти с мрежовата и информационната сигурност.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Вътрешните правила регламентират реа за подаване на сигнали за настъпили и възможни събития, застрашаващи мрежовата и информационната сигурност. Вътрешните правила съдържат информация за лицата, които са отговорни за воденето на регистър на инцидентите, както и реда за регистриране на сигнала, проверката на неговата достоверност, класифицирането му, определянето на приоритет, както и подаването на обратна връзка към подателя на сигнала.

Във вътрешните правила отражение следва да намерят и процедурите за уведомяване за инцидента в неговата йерархическа и функционална ескалация, реда за подаванет на информация за начина за разрешаване на инцидента, както и реда за финализиране на инцидента.

Когато инцидентът е от такова естество, че изисква предприемане на съответни процесуално действия спрямо лице или организаия, вътрешните правила следва да регламентират начина, по които следва да бъдат събрани, съхранени и предадени съответните доказателства.

Вътрешните правила също така съдържат информация относно правото на достъп до регистъра на инцидентите и реда за осъществяването на достъп до него.

Административният орган, съответно ръководителят на субекта следва да разработ планове за справяне с по-сериозните инциденти върху мрежовата и информационната сигурност, както и периодично да ги поддържа и актуализира.

Плановете съдържат информация за:

- отговорника за организацията при настъпване на инцидент;
- реда за информиране;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- мерките, които следва да се предприемат и отговорното за това лице;
- реда за консултиране;
- реда за следене на параметрите по време на инцидента;
- лицето, което ще събира и съхранява необходимата информация, и др.

Административният орган, съответно ръководителят на субекта разработва и приема стратегия за комуникация, която регламентира реда за споделяне на информацията за инцидента със служители, партньори, доставчици, клиенти, медии, държавни органи.

➢ **Уведомяване за инциденти**

В случай на инцидент с мрежовата и информационната сигурност служителят или административния отдел, отговорно за МИС уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите при определените в Закона за киберсигурност срокове.

За уведомяването се попълва форма по следния образец, който при необходимост може да бъде допълван:

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към секторния ЕРИКС

Необходима информация	**Детайли**	**Данни**
(до 2 часа)		
Лице, подаващо уведомлението	Име, фамилия	
Вашият телефонен номер	(GSM)	
Вашата електронна поща		
Организация	Наименование на организацията, засегната от инцидента	
Лице за контакт (за целите на разрешаването на инцидента)	Име, телефонен номер и електронна поща на компетентно лице от предприятието, което при необходимост може да подаде допълнителна информация	
Дата и час	Вписват се датата и часът на възникване на	

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към секторния ЕРИКС

Необходима информация	Детайли	Данни
	инцидента, ако не е възможно - датата и часът на откриването му	
Тип на инцидента		0 Virus 0 Trojan 0 Botnet 0 Dos/DDos 0 Malware 0 Port Scan 0 Spam 0 Phishing 0 Pharming 0 Probe 0 Crack 0 Copyright 0 Ransomware 0 Defacement 0 Exploiting known Vulnerabilities 0 Application Compromise 0 Login Attempts 0 SQL injections 0 Unknown 0 Other
Кратко описание на инцидента	Вписва се кратко описание на инцидента,	

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към секторния ЕРИКС

Необходима информация	Детайли	Данни
	като се включва всяка практическа/техническа информация (тази информация се предоставя, в случай че е налична)	
Трансгранично въздействие	• Вписва се информация за евентуално трансгранично въздействие и се посочват държавите • Вписва се информация за услугите, които са засегнати	
Въздействие върху други съществени услуги	Вписва се информация на кои други	

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към секторния ЕРИКС

Необходима информация	Детайли	Данни
	съществени услуги евентуално ще окаже въздействие	
Засегната система (попълва се, ако е налична информацията)	IP Address: DNS: Operating System:	
Източник на атаката (попълва се, ако е налична информацията)	IP Address: DNS:	
Предприети действия	Описват се първоначалните действия, предприети до момента - до 2 часа от засичането на инцидента	
Публично оповестяване	Съгласно комуникационна	

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към секторния ЕРИКС

Необходима информация	**Детайли**	**Данни**
	стратегия на администрацията	
до 5 работни дни		
Механизъм на атаката	Описва се механизмът на атаката	
Предприети действия	Описват се подробно действията, предприети за разрешаване на инцидента	
Необходимост от коригиращи действия	Има ли необходимост от промяна в настройките на защитните стени, WAF или др. Промяна на политиката за сигурност, ако се налага	

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ

към секторния ЕРИКС

Необходима информация	Детайли	Данни
	Обучение на персонала	
Анализ на артефаки	Описват се резултатите от анализа на артефактите, ако има установени такива, и инструментите, използвани за това. Изпраща се копие от артефактите	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията	

Секторните екипи за реагиране при инциденти с компютърната сигурност съставя и изпраща обобщена информация относно инцидента към CERT Bulgaria (Националния екип за реагиране при инциденти с компютърната сигурност) [15], като за

[15] https://www.govcert.bg/BG/Pages/default.aspx

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

това се използва специално разработен образец.

ОБОБЩЕНА СТАТИСТИЧЕСКА ИНФОРМАЦИЯ ЗА ИНЦИДЕНТИ

от секторния ЕРИКС към националния ЕРИКС

	I/II/III/IV тримесечие за текущата година	Общо за текущата година
Получени сигнали		
Засегнати IP адреси		
Изпратени мейли		
Регистрирани на сайта		

Не всички сигнали се регистрират като инциденти

Приоритет на регистрираните инциденти	I/II/ III/IV тримесечие за текущата година	Общо за текущата година
Висок		
Среден		
Нисък		
Общо	0	0

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Определянето на приоритета на инциденти се извършва съгласно приложение № 7

Видове инциденти	I/II/III/IV тримесечие за текущата година	Общо за текущата година
Fraud		
Malicious code		
Abusive Content (Spam)		
Availability (DDoS)		
Intrusion Attempts		
Information Gathering		
Intrusions		
Information Security		
Vulnerable		
Other		
Botnet		
Общо:	0	0

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Класификацията на инцидентите се извършва съгласно таксономията на ENISA, посочена в приложение № 7

Засегнати IP адреси по видове инциденти	I/II/III/IV тримесечие за текущата година	Общо за текущата година
Fraud		
Malicious code		
Spam		
Botnet		
Availability (DDoS)		
Intrusion Attempts		
Information Gathering		
Intrusions		
Vulnerable		
Other		
Засегнати IP адреси	0	0

- **Резервиране и архивиране на информация**

Всички посочени по- горе в изложениерто вътрешни правила и инструкции следва да бъдат разработени в пълно съответствие с целите и стратегическите насоки, определени в националните политики за мрежова и информационна сигурност във връзка с интегритета на информацията и личните данни, в случай на инцидент.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Във вътрешните правила и инструкции следва да намерят регламентация процесите и отговорните лица за резервиране и архивиране на информация, като трябва задължително да бъде уточнено коя точно информация (бази данни, имиджи на системи и др.) ще подлежи на резервиране и/или архивиране, по какъв начин ще бъде извършвано архивирането и резервирането, дали това ще бъде напълно или частично, като в случай, че бъде частично, то точно кои части подлежат на архивиране и резервиране.

В регламентацията следва да бъде отразено ясно и точно периодите на извършване на архивирането и резервирането, а също така и броят на копията, времето и мястото за тяхното съхранение. Не на последно място на регламентация подлежи и кръга от лица, които са натоварени с отговорности по резервиране и архивиране на информацията, както и начините и условията, при които резервираната/архивираната информация може да бъде използвана.

При резервиране и/или архивиране на информацията следва да се съблюдават някои изисквания, а именно:

- да се правят регулярни копия съобразно риска от загуба на информация и динамиката на изменението ѝ;
- копията на информация да са отбелязани по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час;
- копията на чувствителна информация да са в криптиран вид или поне защитени с парола;

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- копията на информацията да се съхраняват на отделна машина и по възможност в друга защитена мрежа;

- едно от копията на критична за дейността информация се съхранява off-line и по възможност в друга сграда или на отдалечено място;

- да се прави регулярна проверка на годността на резервните копия, дали те изпълняват целите, за които са създадени, и постига ли се необходимото време за възстановяване.

➢ **Резервиране на компоненти на инфраструктурата**

Административният орган, съответно ръководителят на субекта следва да предприеме подходящи и съответни на рисковете мерки за гарантиране на нивото на услигите и дейностите, като резервиране на системи и устройства; балансиране на натоварването на критични устройства или системи; резервиране на центрове за данни.

- **Планове за непрекъсваемост**

Административният орган, съответно ръководителят на субекта разработва планове за действие в случай на авария, природно бедствие или други непредвидени обстоятелства, които са от естество да прекъснат предоставяната от него услуга. Административният орган, съответно ръководителят на субекта определя служиели, отговорни за изпълнение на плановете в случай на настъпване на някоя от предпоставките за тяхното активиране.

Плановете следва регулярно да бъдат разигравани, с оглед установяване на актуалност, адекватност и реална приложимост, както и с оглед поддържането на

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

готовност у лицата, които са отговорни за тяхното изпълнение

IX. КОНТРОЛ

Контролът по спазване на изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност се осъществява чрез одити, проверки и анкети.

1. Одити:

Одитите могат да бъдат три вида: вътрешни, организирани от самия административен орган, съответно ръководител на субект, външни, организирани от клиенти или доставчици на органа/ субекта, или такива, провеждани от независими организации, занимаващи се с одит, които действат като контролни органи на изпълнителната власт или пък от организации, извършващи акредитация и/или сертификация.

Одити следва да се извършват периодично, като препоръчителният им интензитет е веднъж в годината. Одитът задължително се провежда по предварително разработен протокол (процедура), така че лицата да имат предвидимост за това на какви очаквания следва да отговорят. Лицето, осъществяващо одита следва да притежава специфична квалификация в областта на контрола и да притежава необходимите знания и професионален опит в областта на мрежовата и информационната сигурност, с оглед гарантирането на компетентното извършване на одита.

В областта на мрежовата и информационната сигурност действа принципът че одиторът не може да одитира собствената си дейност, с оглед на което одитори следва да бъдат независими лица.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Резултатите от извършения одит трябва да бъдат описани подробно писмено и да бъдат сведени до знанието на служителя, който отговаря за съответната област, която е подложена на одит.

В случай, че бъде установено несъответствие с изискванията, следва да бъде описано подробно какво е несъответствието и с кое конкретно изискване е констатирано, както и да бъде предотавен срок за неговото привеждане в съответствие с изискванията.

След приключване на одитната дейност, резултатите се предотавят на съответния национален компетентен прган по чл. 16, ал. 5 от Закона за киберсигурност. Ангажиментът за предоставяне на тази информация е на административния орган, съответно ръководителя на субекта.

2. Проверки:

Проверки за оценка на съответствието с изискванията за минимални мерки за мрежова и информационна сигурност са в прерогатива на Министъра на електронното управление.

Проверките се извършват по предварително разписани и приети от Министъра на електронното управление вътрешни правила. Проверките се планират по годишна програма, която също е одобрена от Министъра на електронното управление и е публична на страницата на Министерство на електронното управление[16].

Проверки извън одобрената програма могат да се извършват само по

[16] https://e-gov.bg/wps/portal/agency/strategies-policies/network-security/mis-annual-program

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

искане на правоимащ орган или по искане на самия субект, като те се планират и извършват само при наличие на възможност за това предвид ангажираността на оправомощените лица.

За всяка проверка следва да бъде създаден план, който се свежда до знанието на административния орган, съответно ръководителя на субекта, който ще бъде проверяван. Времето на извършване на проверката следва да бъде съгласуван с административния орган, съответно с ръководителя на субекта най- малко 7 дни преди началната дата на проверката.

Подобно на лицата, осъществяващи одити и лицата, натоварени с извършване на проверките следва да притежават специална квалификация в областта на контрола, както и да притежават необходимите знания и професионален опит в областта на мрежовата и информационната сигурност.

Резултатите от извършената проверка се документират в доклад, който следва да бъде изготвен в срок до 10 дни от приключване на проверката. В доклада следва да бъде посочена оценката на мрежовата и информационната сигурност на проверявания орган/субект, а при установяване на несъответствие с изискванията, то следва да бъде подробно описано в какво се състои несъответствието и с кое точно изискване е то, да бъдат дадени насоки и препоръки за отстраняването му, както и да бъде определен подходящ срок за привеждане в съответствие с изискванията за мрежова и информационна сигурност.

Проверяващите лица притежават правомощията да дават препоръки за повишаване на общото ниво и състояние на мреждова и информационна сигурност на проверявания орган/субект.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

След приключване на проверката и съставяне на доклада, той се изпаща на проверявания административен орган, съответно ръководител на субект за сведение и изпълнение. Министърът на електронното управление лично или чрез упълномощено лице следва да планира извършването на последващ контрол за изпълнение на дадените препоръки, като за тях отново следва да бъде извършено уведомяване на съответния административен орган/ръководител на субект.

3. Анкети

Съобразно предвиденото в Закона за киберсигурност националните компетентни органи използват анкети, с които извършват оценка дали административните органи, операторите на съществени услуги и доставчиците на цифрови услуги изпълняват задълженията си във връзка с минималните изисквания за мрежова и информационна сигурност. Анкетите дават информация и относно въздействието на изпълнението на задълженията върху мрежовата и информационна сигурност като по този начин дават отправна точка за това какви действия следва да бъдат предприети в случай на неизпълнение.

X. Препоръчителни функции на служителя/звеното, отговарящо за мрежовата и информационната сигурност, съгласно Приложение № 6 към чл. 3, ал.2, т. 2 от Наредбата за минималните изисквания за мрежова и информационна сигурност:

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в политиката на органа/субекта.

2. Участва в изготвянето на политиките и документираната информация.

3. Следи за спазването на вътрешните правила, инструкциите и

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност.

4. Консултира ръководството на органа/субекта във връзка с информационната сигурност.

5. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност.

6. Периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в административното звено и ги представя на ръководителя.

7. Координира обученията, свързани с мрежовата и информационната сигурност.

8. Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства. Анализира резултатите от тях и организира изменение на плановете, ако е необходимо.

9. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.

10. Следи за акуратното водене на регистъра на инцидентите.

11. Уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 (уведомяване за инциденти) от тази наредба.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

12. Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.

13. Следи за актуализиране на използвания софтуер и фърмуер.

14. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им.

15. Организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им.

16. Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган.

17. Предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

Списък на стандарти в областта на мрежовата и информационната сигурност:

- ***Стандарти за управление на сигурността на информацията:***

БДС EN ISO/IEC 27000 - Информационни технологии - Методи за сигурност - ***Системи за управление на сигурността на информацията - Общ преглед и речник***

БДС EN ISO/IEC 27001 - Информационни технологии - Методи

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

за сигурност - ***Системи за управление на сигурността на информацията – Изисквания***

БДС EN ISO/IEC 27002 - Информационни технологии - Методи за сигурност - ***Кодекс за добра практика за управление на сигурността на информацията***

БДС ISO/IEC 27003 - Информационни технологии - Методи за сигурност - ***Указания за внедряване на системи за управление на сигурността на информацията***

БДС ISO/IEC 27004 - Информационни технологии - Методи за сигурност - ***Управление на сигурността на информацията - Наблюдение, измерване, анализ и оценяване***

ISO/IEC 27009 - Information technology - Security techniques - ***Sector-specific application of ISO/IEC 27001 - Requirements*** (Информационни технологии - Техники за сигурност - ***Специфично за секторите прилагане на ISO/IEC 27001 - Изисквания)***

БДС ISO/IEC 27013 - Информационни технологии - Методи за сигурност - ***Указания за съвместно внедряване на ISO/IEC 27001 и ISO/IEC 20000-1***

ISO/IEC 27014 - Information technology - Security techniques - ***Governance of information security*** (Информационни технологии - Методи за сигурност - ***Управление на сигурността на информацията)***

ISO/IEC 27017 - Information technology - Security techniques - ***Code of***

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

practice for information security controls based on ISO/IEC 27002 for cloud services (Информационни технологии - Методи за сигурност - ***Кодекс за добра практика за контрол на сигурността на информацията за облачни услуги, базиран на ISO/IEC 27002)***

ISO/IEC 29146 - Information technology - Security techniques - ***A framework for access management*** (Информационни технологии - Методи за сигурност - ***Рамка за управление на достъпа)***

БДС ISO/IEC 27018 - Информационни технологии - Методи за сигурност - ***Кодекс за добра практика за защита на лични данни (personally identifiable information PII) в обществени облаци, действащи като администратори на PII***

- ***<u>Стандарти за управление на риска:</u>***

БДС ISO/IEC 27005 - Информационни технологии - Методи за сигурност - ***Управление на риска за сигурността на информацията***

БДС ISO 31000 - Управление на риска – ***Указания***

БДС EN 31010 - Управление на риска - ***Методи за оценяване на риска***

ETSI TS 102 165-1 - CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) (КИБЕР; ***Методи и протоколи;*** Част 1: Методика и професионална форма на заплаха, уязвимост, анализ на риска (Threat, Vulnerability, Risk Analysis (TVRA)

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

- ***Стандарти за идентификация и автентикация***

ISO/IEC 11770-1 - Information technology - Security techniques - ***Key management*** - Part 1: Framework (Информационни технологии - Методи за сигурност - ***Управление на ключовете*** - Част 1: Рамка)

ISO/IEC 11770-2 - Security techniques - ***Key management*** - Part 2: Mechanisms using symmetric techniques (Информационни технологии - Методи за сигурност - ***Управление на ключовете*** - Част 2: Механизми, използващи симетрични техники)

ISO/IEC 11770-3 - Information technology - Security techniques - ***Key management*** - Part 3: Mechanisms using asymmetric techniques (Информационни технологии - Методи за сигурност - ***Управление на ключовете*** - Част 3: Споразумение за невидими Diffie-Hellman ключове)

ISO/IEC 11770-4 - Information technology - Security techniques - ***Key management*** - Part 4: Mechanisms based on weak secrets (Информационни технологии - Методи за сигурност - ***Управление на ключовете*** - Част 4: Механизми, основани на слаби тайни)

ISO/IEC 11770-5 - Information technology - Security techniques - ***Key management*** - Part 5: Group key management (Информационни технологии - Методи за сигурност - ***Управление на ключовете*** - Част 5: Управление на групови ключове)

ISO/IEC 11770-6 - Information technology - Security techniques - ***Key management*** - Part 6: Key derivation (Информационни технологии - Методи

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

за сигурност - ***Управление на ключовете*** - Част 6: Деривация на ключове)

ISO/IEC 20889 - Privacy enhancing data de-identification terminology and classification of techniques (Технологии за защита на личните данни от де-идентификация, терминология и класификация на техниките)

ISO/IEC 24760-1 - Information technology - Security techniques - ***A framework for identity management*** - Part 1: Terminology and concepts (Информационни технологии - Методи за сигурност - ***Рамка за управление на идентичността*** - Част 1: Терминология и понятия)

ISO/IEC 24760-2 - Information technology - Security techniques - ***A framework for identity management*** - Part 2: Reference architecture and requirements (Информационни технологии - Методи за сигурност - ***Рамка за управление на идентичността*** - Част 2: Препоръчителна архитектура и изисквания)

ISO/IEC 24760-3 - Information technology - Security techniques - ***A framework for identity management*** - Part 3: Practice (Информационни технологии - Методи за сигурност - ***Рамка за управление на идентичността*** - Част 3: Прилагане)

ISO/IEC 29115 - Information technology - Security techniques - ***Entity authentication assurance framework*** (Информационни технологии - Методи за сигурност - ***Рамка за гарантиране на автентичността на субекти)***

ISO/IEC 29151 - Information technology - Security techniques - **Code of practice for personally identifiable information protection** (Информационни технологии - Техники за сигурност - ***Кодекс на практики за защита на личната информация)***

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ISO/IEC 29191 - Information technology - Security techniques - ***Requirements for partially anonymous, partially unlinkable authentication*** (Информационни технологии - Техники за защита - ***Изисквания за частично анонимно удостоверяване, частична псевдоминизация***)

ISO/IEC 18370-1 - Information technology - Security techniques - ***Blind digital signatures*** - Part 1: General (Информационни технологии - Методи за сигурност - ***Невидими цифрови подписи*** - Част 1: Общи положения)

ISO/IEC 18370-2 - Information technology - Security techniques - ***Blind digital signatures*** - Part 2: Discrete logarithm based mechanisms (Информационни технологии - Методи за сигурност - ***Невидими цифрови подписи*** - Част 2: Механизми, базирани на дискретни логаритми)

ISO/IEC 20008-1 - Information technology - Security techniques - ***Anonymous digital signatures*** - Part 1: General (Информационни технологии - Методи за сигурност - ***Анонимни цифрови подписи*** - Част 1: Общи положения)

ISO/IEC 20008-2 - Information technology - Security techniques - ***Anonymous digital signatures*** - Part 2: Mechanisms using a group public key (Информационни технологии – Методи за сигурност - ***Анонимни цифрови подписи*** - Част 2: Механизми с използване на групов публичен ключ)

ISO/IEC 20009-1 - Information technology - Security techniques - ***Anonymous entity authentication*** - Part 1: General (Информационни технологии - Методи за сигурност - ***Идентификация на анонимни обекти*** - Част 1: Общи положения)

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ISO/IEC 20009-2 - Information technology - Security techniques - ***Anonymous entity authentication*** **-** Part 2: Mechanisms based on signatures using a group public key (Информационни технологии - Методи за сигурност - ***Идентификация на анонимни обекти*** - Част 2: Механизми, основани на подписи с използване на групов публичен ключ)

ISO/IEC 20009-4 - Information technology - Security techniques - ***Anonymous entity authentication*** - Part 4: Mechanisms based on weak secrets (Информационни технологии - Методи за сигурност - ***Идентификация на анонимни обекти*** - Част 4: Механизми, основани на слаби тайни)

- ***Стандарти за криптиране***

ISO/IEC 18033-1 - Information technology - Security techniques - ***Encryption algorithms*** **-** Part 1: General (Информационни технологии - Методи за сигурност - ***Алгоритми за криптиране*** **-** Част 1: Общи положения)

ISO/IEC 18033-2 - Information technology - Security techniques - ***Encryption algorithms*** **-**Part 2: Asymmetric ciphers (Информационна технология - Методи за сигурност - ***Алгоритми за криптиране*** - Част 2: Асиметрични шифри)

ISO/IEC 18033-4 - Information technology - Security techniques - ***Encryption algorithms*** **-** Part 3: Block ciphers (Информационни технологии - Методи за сигурност - ***Алгоритми за криптиране*** - Част 3: Блокови шифри)

ISO/IEC 18033-4 - Information technology - Security techniques - ***Encryption algorithms*** **-** Part 4: Stream ciphers (Информационни технологии - Методи за сигурност - ***Алгоритми за криптиране*** - Част 4: Поточни шифри)

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ISO/IEC 18033-5 - Information technology - Security techniques - ***Encryption algorithms*** - Part 5: Identity-based ciphers (Информационни технологии - Методи за сигурност - ***Алгоритми за криптиране*** - Част 5: Шифри, базирани на идентичност)

- ***Стандарти за одити***

ISO/IEC 27006 - Information technology - Security techniques - ***Requirements for bodies providing audit and certification of information security management systems*** (Информационни технологии - Методи за сигурност - ***Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията***)

ISO/IEC 27007 - Information technology - Security techniques - ***Guidelines for information security management systems auditing*** (Информационни технологии - Методи за сигурност - ***Указания за одит на системи за управление на сигурността на информацията*** - допълнение към насоките, съдържащи се в стандарт ISO 19011)

БДС EN ISO 19011 - ***Указания за извършване на одит на системи за управление***

БДС EN ISO/IEC 17020 - Оценяване на съответствието - ***Изисквания за дейността на различни видове органи, извършващи контрол***

- ***Стандарти за оценка на сигурността***

ISO/IEC 15408-1 - Information technology - Security techniques - ***Evaluation criteria for IT security*** - Part 1: Introduction and general model

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

(Информационни технологии - Методи за сигурност - ***Критерии за оценка на ИТ сигурността*** - Част 1: Въведение и общ модел)

ISO/IEC 15408-2 - Information technology - Security techniques - ***Evaluation criteria for IT security*** - Part 2: Security functional components (Информационни технологии - Методи за сигурност - ***Критерии за оценка на ИТ сигурността*** - Част 2: Функционални компоненти за сигурност)

ISO/IEC 15408-3 - Information technology - Security techniques - ***Evaluation criteria for IT security*** - Part 3: Security assurance components (Информационни технологии - Методи за сигурност - ***Критерии за оценка на ИТ сигурността*** - Част 3: Компоненти за осигуряване на сигурност)

ISO/IEC 18045 - Information technology - Security techniques - ***Methodology for IT security evaluation*** (Информационни технологии - Методи за сигурност - ***Методология за оценка на ИТ сигурността)***

ISO/IEC TS 19608 - ***Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*** (***Указания за разработване на функционални изисквания за сигурност и неприкосновеност, основани на ISO/IEC 1540)***

ISO/IEC TR 20004:2015 - Information technology - Security techniques - ***Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*** (Информационни технологии - Методи за сигурност - ***Усъвършенстване на анализа на софтуерните уязвимости в съответствие с ISO/IEC 15408 и ISO/IEC 18045)***

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ISO/IEC 29134 - Information technology - Security techniques - ***Guidelines for privacy impact assessment*** (Информационни технологии - Методи за сигурност - ***Указания за оценка на въздействието върху неприкосновеността на личните данни***)

ISO/IEC 29190 - Information technology - Security techniques - ***Privacy capability assessment model*** (Информационни технологии - Методи за сигурност - ***Модел за оценка на способността за защита на личните данни***)

- ***Стандарти за сигурност, които са в етап на разработване през 2019 г.***

ISO/IEC CD 20009-3 - Information techno-logy - Security techniques - **Anonymous entity authentication** - Part 3: Mechanisms based on blind signatures concepts (Информационни технологии - Методи за сигурност - ***Идентификация на анонимни обекти*** - Част 3: Механизми, основани на концепции за скрити подписи)

ISO/IEC 27551 - Information technology - Security techniques - ***Requirements for attribute-based unlinkable entity authentication*** (Информационни технологии - техники за сигурност - ***Изисквания за удостоверяване на субекти на базата на несвързващи атрибути***)

ISO/IEC PDTR 27550 - Information techno- logy - Security techniques - ***Privacy engineering*** (Информационни технологии - Техники за сигурност - ***Инженеринг на лични данни***)

ISO/IEC DIS 27552 - Security techniques - ***Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*** - Requirements and guidelines (Методи за сигурност - ***Разширяване на ISO/IEC 27001 и ISO/IEC 27002 за управление***

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

на личната информация - Изиск- вания и насоки)

ISO/IEC 27030 - Information technology - Security techniques - Guidelines for security and privacy in Internet of Things (IoT) (Информационни технологии - Методи за сигурност - ***Указания за сигурност и неприкосновеност на личните данни в Интернет на нещата (IoT)***

ISO/IEC 29184 - Information technology - ***Online privacy notices and consent*** (Информационни технологии - ***Съобщения и съгласие за поверителност в интернет)***

Забележка. Номерата на стандартите са уникални и еднозначно свързани с техните имена. Пред номера на стандарта се изписват абревиатурите на организациите, които са го одобрили. След номера на стандарта се изписва годината, в която той е приет. Общото изписване е от вида ISO/IEC 27001:2013 или БДС ISO/IEC 27001:2018, като в случая става въпрос за един и същ стандарт.

Стандартите се преглеждат от съответните организации и при необходимост се актуализират на всеки пет години, като новата версия отменя действието на предишната.

XI. ЗАКЛЮЧЕНИЕ: Новите предизвикателства пред националната нормативна уредба

С приемането на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2), се прави опит за хармонизация на изискванията за киберсигурност и мерките за мрежова и

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

информационна сигурност.

Новата директива предвижда официалното създаване на Европейската мрежа за връзка на организациите при киберкризи – EU-CyCLONe, която ще подпомага координираното управление на мащабни инциденти и кризи в областта на киберсигурността.

За разлика от досегашната регулация, която предвиждаше всяка държава- членка да определи кои субекти следва да отговарят на критериите, за да бъдат определени като оператори на съществени услуги, новата Директива определя, че всички средни и големи субектри, които извършват своята дейност в обхвата на Директивата или предоставят услуги в този обхват, ще попаднат в нейното приложно поле. Това означава, че кръгът от субекти се разширява на база числеността на служителите в съответния субект.

Някои области са категорично изключени от обхвата на Директивата, като това са отбраната и националната сигурност, обществената сигурност и правоприлагането в лицето на съдебната власт, както и парламентите.

Новата Директива ще се прилага за публичните администрации на централно и регионално равнище, като в правомощията на държавите- членки ще бъде поставено да решат дали тя да се прилага за субекти на местно ниво.

Новата Директива рационализира задълженията за докладване, за да се оптимизират процесите във връзка с докладването на инциденти, както и за са се облекчат субектите в това направление.

Новата Директива ще наложи извършването на промени в Закона за

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

киберсигурност и съответните подзаконови нормативни актове. Новата Директива ще наложи промени и в Закона за електронните съобщения, както и в други секторни политики.

България разполага с време до 17.10.2024 г да транспонира новата Директива в своето законодателство.

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Използвани източници:

НАЦИОНАЛНИ ДОКУМЕНТИ:

ЗАКОН ЗА КИБЕРСИГУРНОСТ (Обн. ДВ. бр.94 от 13 Ноември 2018г., изм. ДВ. бр.69 от 4 Август 2020г., изм. и доп. ДВ. бр.85 от 2 Октомври 2020г., изм. и доп. ДВ. бр.15 от 22 Февруари 2022г., изм. ДВ. бр.25 от 29 Март 2022г.)

ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ (Обн. ДВ. бр.46 от 12 Юни 2007г., изм. ДВ. бр.82 от 16 Октомври 2009г., изм. ДВ. бр.20 от 28 Февруари 2013г., доп. ДВ. бр.40 от 13 Май 2014г., изм. ДВ. бр.13 от 16 Февруари 2016г., изм. и доп. ДВ. бр.38 от 20 Май 2016г., изм. и доп. ДВ. бр.50 от 1 Юли 2016г., доп. ДВ. бр.62 от 9 Август 2016г., доп. ДВ. бр.98 от 9 Декември 2016г., изм. ДВ. бр.88 от 23 Октомври 2018г., изм. и доп. ДВ. бр.94 от 13 Ноември 2018г., изм. и доп. ДВ. бр.94 от 29 Ноември 2019г., доп. ДВ. бр.102 от 31 Декември 2019г., изм. ДВ. бр.69 от 4 Август 2020г., доп. ДВ. бр.85 от 2 Октомври 2020г., изм. и доп. ДВ. бр.15 от 22 Февруари 2022г.)

ЗАКОН ЗА ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ (Обн. ДВ. бр.38 от 20 Май 2016г., изм. ДВ. бр.50 от 1 Юли 2016г., изм. и доп. ДВ. бр.101 от 20 Декември 2016г., изм. ДВ. бр.97 от 5 Декември 2017г., изм. ДВ. бр.14 от 13 Февруари 2018г., изм. ДВ. бр.1 от 3 Януари 2019г., изм. ДВ. бр.58 от 23 Юли 2019г., изм. ДВ. бр.94 от 29 Ноември 2019г., изм. ДВ. бр.60 от 7 Юли 2020г., изм. ДВ. бр.15 от 22 Февруари 2022г.)

НАРЕДБА ЗА МИНИМАЛНИТЕ ИЗИСКВАНИЯ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, в сила от 26.07.2019 г., Приета с ПМС № 186 от 19.07.2019 г. (Обн. ДВ. бр.59 от 26 Юли 2019г., изм. ДВ. бр.36 от 13 Май 2022г., изм. ДВ. бр.47 от 24 Юни 2022г.)

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

НАРЕДБА ЗА ОБЩИТЕ ИЗИСКВАНИЯ КЪМ ИНФОРМАЦИОННИТЕ СИСТЕМИ, РЕГИСТРИТЕ И ЕЛЕКТРОННТЕ АДМИНИСТРАТИВНИ УСЛУГИ (В сила от 01.03.2017 г., Приета с ПМС № 3 от 09.01.2017 г., Обн. ДВ. бр.5 от 17 Януари 2017г., изм. ДВ. бр.66 от 10 Август 2018г., изм. и доп. ДВ. бр.4 от 14 Януари 2020г., изм. ДВ. бр.47 от 24 Юни 2022г.)

АДМИНИСТРАТИВНОПРОЦЕСУАЛЕН КОДЕКС (Обн. ДВ. бр.30 от 11 Април 2006г., изм. ДВ. бр.59 от 20 Юли 2007г., изм. ДВ. бр.64 от 7 Август 2007г., изм. ДВ. бр.94 от 31 Октомври 2008г., изм. ДВ. бр.35 от 12 Май 2009г., изм. ДВ. бр.100 от 21 Декември 2010г., изм. ДВ. бр.39 от 20 Май 2011г., изм. ДВ. бр.77 от 9 Октомври 2012г., изм. и доп. ДВ. бр.104 от 3 Декември 2013г., изм. и доп. ДВ. бр.27 от 25 Март 2014г., изм. и доп. ДВ. бр.74 от 20 Септември 2016г., доп. ДВ. бр.13 от 7 Февруари 2017г., изм. ДВ. бр.58 от 18 Юли 2017г., доп. ДВ. бр.63 от 4 Август 2017г., изм. ДВ. бр.85 от 24 Октомври 2017г., доп. ДВ. бр.103 от 28 Декември 2017г., доп. ДВ. бр.42 от 22 Май 2018г., изм. ДВ. бр.65 от 7 Август 2018г., изм. и доп. ДВ. бр.77 от 18 Септември 2018г., изм. ДВ. бр.36 от 3 Май 2019г., изм. и доп. ДВ. бр.94 от 29 Ноември 2019г., доп. ДВ. бр.44 от 13 Май 2020г., изм. и доп. ДВ. бр.98 от 17 Ноември 2020г., изм. ДВ. бр.9 от 2 Февруари 2021г., изм. и доп. ДВ. бр.15 от 19 Февруари 2021г., доп. ДВ. бр.102 от 23 Декември 2022г.)

Националната стратегия за киберсигурност “Киберустойчива България 2020”.

АКТУАЛИЗИРАНА националната стратегия „Киберустойчива България 2023 г“

Проект на Пътна карта към актуализирана Национална стратегия за киберсигурност „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023”

Методика и правила за извършване на оценка за съответствието с мерките за мрежова и информационна сигурност

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

ЕВРОПЕЙСКИ ДОКУМЕНТИ:

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

Регламент (ЕС) 2018/1724 на Европейския парламент и на Съвета от 2 октомври 2018 година за създаване на единна цифрова платформа за предоставяне на достъп до информация, до процедури и до услуги за оказване на помощ и решаване на проблеми и за изменение на Регламент (ЕС) № 1024/2012

Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО

Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Директива (ЕС) 2022/2555 на Европейския парламетн и на Съвета от 14.12.2022 г относно мерките за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/172 и за отмяна на Директива (ЕС) 2016/1148

Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации)

Стратегия на ЕС за Съюза на сигурност с обхват 2020- 2025 г

ИНТЕРНЕТ СТРАНИЦИ:

https://eur-lex.europa.eu/homepage.html?locale=bg

https://www.nsi.bg/bg

https://saveti.government.bg/web/cc_1901/1

https://unifiedmodel.egov.bg/wps/portal/unified-model/home

https://www.govcert.bg/BG/Pages/default.aspx

https://egov.bg/wps/portal/egov/nachalo

https://www.govcert.bg/BG/Pages/default.aspx

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Използвани съкращения:

На български език:

ЕС- Европейски съюз

НАТО – Организация на Северноатлантическия договор, на английски език „North Atlantic Treaty Organization" (NATO)

ЕРИКС - Екипи за реагиране при инциденти с компютърната сигурност

ОСУ - оператори на съществени услуги

НКО - национални компетентни органи

МИС – Мрежова и информационна сигурност

ДАЕУ- Държавната агенция "Електронно управление"

ЗЕУ – Закон за електронното управление

ПМС- Постановление на Министерски съвет;

ЕПДЕАУ Единен портал за достъп до електронни административни услуги

МИС- Мрежова и информационна сигурност

ОРЗД – Общ регламент за защита на данните, на английски език General data protection Regulation (GDPR)

ЕИЗ – Европейска икономическа зона, преди Европейско икономическо пространство (ЕИП)

НАП- Национална агенция по приходите

НСИ- Национален статистически институт

НКОМКС - Национална координационно-организационна мрежа за киберсигурност

НКСЦ - Национален киберситуационен център

МЕУ – Министерство на електронното управление

МО- Министерство на отбраната

ГДБОП към МВР – Главна Дирекция „Борба с организираната престъпност" към

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

Министерство на вътрешните работи

КИС на МВР – Дирекция Комуникационни и информационни системи на Министерство на вътрешните работи

ДАНС – Държавна агенция „Национална сигурност”

НСЦ – Национален ситуационен център

ЕК – Европейска комисия

ДХЧО- Държавен хибриден частен облак

АПК – Административнопроцесуален кодекс

ЕАУ – Електронни административни услуги

ОС – Оперативна съвместимост

СОС – Семантична оперативна съвместимост

ЗКС – Закон за киберсигурност

НМИМИС – Наредба за минималните изисквания към мрежовата и информационна сигурност

ИКИ- информационна и комуникационна инфраструктура

EECM - единна електронна съобщителна мрежа

ССЕВ – Система за сигурно електронно връчване

На английски език:

UTC – Coordinated Universal Time

VPN - Virtual Private Network

FTP - File Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

WAP - Web Application Firewall

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.

DNS – Domain Name System

DNSSEC – Domain Name System Security Extensions

dmarc – Domain-based Message Authentication, Reporting and Conformance

SPF - Sender Policy Framework

www.eufunds.bg
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.