МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО, ХРАНИТЕ И ГОРИТЕ
ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО ГОРИТЕ
РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ - БЛАГОЕВГРАД
Благоевград, ул. "Васил Коритаров" № 2, п.код 2700, тел. централа 88 50 09, факс 88 50 04

ЗАПОВЕД

22.2.2021 г.

X РД05-19 - 22.02.2021
Рег. номер

Signed by: Sashko Yordanov Popov

На основание чл. 5, ал.1, т.1. от Устройствения правилник на Регионаните дирекции по горите и чл.3, ал.2 и чл.5, ал.1, т. 6 и т.7 от НМИМИС за минималните изисквания за мрежова и информационна сигурност(НМИМИС), в сила от 26.07.2019 г.

НАРЕЖДАМ:

I. Утвърждавам „Вътрешни правила за мрежова и информационна сигурност" в Регионална дирекция по горите Благоевград приложение към настоящата заповед.

II. Определям главен експерт „Системен администратор" да отговаря пряко за информационната и мрежовата сигурност в РДГ.

III. Главен експерт „Системен администратор" изпълнява функциите регламентирани в Приложение № 6 към чл.3, ал., т.2 от НМИМИС и раздел II от Вътрешните правила одобрени с настоящата заповед.

IV. Отменям всички предходни заповеди, с които са одобрени Вътрешни правила за мрежова и информационна сигурност.

Настоящата заповед да се публикува на интернет страницата на Регионална дирекция по горите Благоевград и да се сведе до знанието на служителите на дирекцията за сведение и изпълнение.

Контролът по изпълнението на заповедта възлагам на заместник директора на Регионална дирекция по горите Благоевград.

22.2.2021 г.

X инж. Сашко Попов

ДИРЕКТОР НА РДГ
инж. Сашко Попов
Signed by: Sashko Yordanov Popov

УТВЪРЖДАВАМ
ДИРЕКТОР
(инж. Сашко Попов)

ВЪТРЕШНИ ПРАВИЛА

ЗА
МРЕЖОВАТА И
ИНФОРМАЦИОННАТА СИГУРНОСТ
В РДГ БЛАГОЕВГРАД

2021 г.

РАЗДЕЛ I

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила имат за цел осигуряването на контрол и управление на работата на информационните системи в РДГ Благоевград.

В този смисъл понятието информационна система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми. Програмните продукти и бази данни могат да бъдат специфични за всяко звено от администрацията или с общо предназначение.

Чл. 2. Потребителите на информационни системи в РДГ Благоевград са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 3. Проектирането и изграждането на информационни и комуникационни системи се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на НМИМИС за минималните изисквания за мрежова и информационна сигурност(НМИМИС) (ДВ, БР. 59 от 19.07.2019 г.)

РАЗДЕЛ II

ФУНКЦИИ И ОТГОВОРНОСТИ НА СИСТЕМНИЯ АДМИНИСТРАТОР В РДГ

Чл.4. Системният администратор на РДГ:

- Участва в изготвянето на политиките и документираната информация.
- Следи за спазването на вътрешните правила и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност.
- Консултира ръководството във връзка с информационната сигурност.
- Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност.
- Ежегодно до 31 март изготвя доклад за състоянието на мрежовата и информационната сигурност в РДГ и ги представя на директора.
- Координира обученията, свързани с мрежовата и информационната сигурност.
- Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.
- Следи за акуратното водене на регистъра на инцидентите.
- Уведомява директора на РДГ за възникнали инциденти с компютърната сигурност с цел своевременна реакция на инциденти в съответствие с изискването на чл. 31, ал. 1 от НМИМИС.
- Извършва 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.
- Следи за актуализиране на използвания софтуер и фърмуер.
- Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им.
- Извършва тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им.
- Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган.
- Докладва на директора на РДГ при констатиране на случаи на нарушаване на мерките за мрежовата и информационната сигурност.

Чл. 5. (1) Системния администратор поддържа следната документация:
1. опис на информационните активи – фърмуер и софтуер, който съдържа най малко:
1.1. еднозначна идентификация, като инвентарен, сериен номер или др.;
1.2. основни характеристики;
1.3. услуги, процеси и дейности, в които участва, където е приложимо;
1.4. местоположение;
1.5. година на производство, където е приложимо;
1.6. дата на въвеждане в експлоатация, където е приложимо;
1.7. версия, където е приложимо;
1.8. местонахождение на свързаната с него документация (техническа, експлоатационна, потребителска и др.);
1.9. отговорно лице.
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, 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.
(2) Документацията по ал. 1 трябва да е:
1. еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др.;
2. поддържана в актуално състояние, като се преразглежда и при необходимост се обновява поне веднъж годишно;
3. одобрена от административен орган, съответно от директора на РДГ;
4. достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.
(3) Поддържа информация, доказваща по неоспорим начин изпълнението на изискванията на НМИМИС.
(4) Поддържа списък на администраторските профили за информационните и комуникационните системи и техните компоненти.

Чл. 6. Управление на риска
(1) Системният администратор в РДГ извършва анализ и оценка на риска за мрежовата и информационната сигурност регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите изпълнявани от служителите на РДГ свързани с използване на компютърните системи.
(2) Анализът и оценката на риска се документират и са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.
(3) За анализ и оценка на риска се прилага препоръчителна методика съгласно *Приложение № 1* към настоящите вътрешни правила.
(4) На основание на анализа и оценката на риска се изготвя план за намаляване на неприемливите рискове, който да включва минимум:
1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. необходими ресурси за изпълнение на тези мерки;
3. срок за прилагане на мерките;
4. отговорни лица.

(5) Системния администратор сменя паролите за автентикация на администраторските профили задължително:
1. периодично - най-малко веднъж в годината;
2. при прекратяването на договорните отношения със служители или трети страни, на които тези данни са били известни;
3. при пробив в мрежовата и информационната сигурност.

РАЗДЕЛ III
ПРАВИЛА ЗА ПРИДОБИВАНЕ, ВЪВЕЖДАНЕ В ЕКСПЛОАТАЦИЯ, ПРЕМЕСТВАНЕ, ИЗВЕЖДАНЕ ОТ ЕКСПЛОАТАЦИЯ И УНИЩОЖАВАНЕ НА ИНФОРМАЦИОННИ АКТИВИ

Чл.7. Компютърните системи и софтуер за нуждите на РДГ се придобиват, съгласно Вътрешните правила за придобиване на ДМА в РДГ, при спазване на всички изисквания на СФУК.

Чл.8. (1) Компютърните системи и софтуер се въвеждат в експлоатация от системния администратор на РДГ или оправомощено лице на доставчика при спазване на всички изисквания на НМИМИС, за което се съставя протокол.

(2) Преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив.

Чл.9. (1) Компютърните системи и софтуер се извеждат от експлоатация от системния администратор на РДГ или оправомощено лице на доставчика при спазване на всички изисквания на НМИМИС, за което се съставя протокол.

(2) При извеждането от експлоатация на носители, съдържащи информация необходима за функциониране на системите на РДГ, същата се архивира по правилата на Раздел IX.

(3) Носителите и информацията на тях се унищожава по начин, който гарантира че информацията няма да може да бъде извлечена от неупълномощени лица. Физическото унищожаване на информационните носители става със счупване или чрез машинно унищожаване. Предварително се проверяват, за да е сигурно, че необходимата информация е копирана и след това цялата информация е изтрита от тях преди унищожаване.

(4) Компютърните конфигурации и фърмуер се бракуват от комисия назначена от директора на РДГ при спазване на общите правила за бракуване на ДМА, след което се предоставят на специализирани фирми за разкомплектоване и рециклиране на електронно оборудване.

РАЗДЕЛ IV
КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Чл.10. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:

(1) разделяне на потребителски от администраторски функции;

(2) установяване на нива и достъп до информация;

(3) регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;

(4) осъществяването на контрол от специализирани звена и служители на администрацията.

Чл. 11. (1). Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили;

(2) Нивото на достъп (до кои модули/масиви) на даден служител се разрешава по предложение на прекия ръководител, одобрено от директора на РДГ.

(3) Служителите, имащи право да заявяват даване, променяне и спиране на достъп,

правят редовни прегледи на достъпите, но не по-рядко от веднъж в годината

(4) При прегледите по ал.3 се установява дали всички, на които е даден достъп до мрежата, до отделните системи и/или приложения, имат право на него в съответствие със служебните им задължения, дали външни лица имат достъп и какъв е той (бивши служители, представители на трети страни);

(5) За целите на прегледите по ал.3 системния администратор на РДГ предоставя списък на всички, които имат достъп до съответните модули/масиви.

(6) Служителите по ал. 2 документирано потвърждават или дават указания за промяна на модулите/масивите, до които на даден служител има достъп.

Чл.12. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва чрез средствата на активна директория с конкретно потребителско име, осигурено от Системния администратор, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 13 (1). Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

(2) При прекратяване на трудовото/служебното правоотношение, служителя по човешки ресурси уведомява за това системния администратор, който преустановява достъпа на лицето до всички модули/масиви до които му е бил предоставен достъп.

(3) При промяна на длъжността на работника/служителя, което налага промяна на нивото на достъп до информационните системи/масиви, това се прави по реда на чл.5, ал.2.

Чл. 14. Лицата, които обработват лични данни, използват уникални пароли с достатъчно сложност, които не се записват или съхраняват онлайн;

(1) Всички пароли за достъп на системно ниво се променят периодично;

Чл. 15. Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Чл. 16. На служителите на РДГ Благоевград, които използват електронни бази данни и техни производни (текстове, разпечатки, карти и скици) се забранява:

(1) да ги изнасят под каквато и да е форма извън служебните помещения преди извеждане от деловодството (извършване на услуга);

(2) да ги използват извън рамките на служебните си задължения;

(3) да ги предоставят на външни лица без да е заявена услуга.

Чл. 17. За нарушение целостта на данните се считат следните действия:

(1) унищожаване на бази данни или части от тях;

(2) повреждане на бази данни или части от тях;

(3) вписване на невярна информация в бази данни или части от тях.

Чл. 18. При изнасяне на носители извън физическите граници на РДГ Благоевград, те се поставят в подходяща опаковка и в запечатан плик.

Чл. 19. На служителите е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 20. Служителите са длъжни да избягват всякакъв риск от достъп до информация от неупълномощени лица, както и до злоумишлен софтуер. Забранено е съобщаването на тайна и чувствителна информация по мобилни телефони на места, където може да стане достъпна за трети страни.

Чл. 21. Събирането, подготовката и въвеждането на данни на страницата се извършва от служител на РДГ Благоевград, определен със заповед на Директор РДГ Благоевград. На посоченото длъжностно лице се създава потребителско име и парола за извършване на актуализациите.

Чл. 22. Събирането и подготовката на данните се извършва от служители в техния

ресор, след което данните се изпращат в електронен вид (на файлове) на служителя отговорен за качването им на интернет страницата на РДГ Благоевград.

РАЗДЕЛ V
РАБОТНО МЯСТО

Чл. 23. Работното място се състои от компютърна техника, периферна техника и комуникационни средства, разположени в работното помещение.

Чл. 24. Работното място се оборудва при спазване на изискванията на Наредба № 7 от 15.08.2005 г. за минималните изисквания за осигуряване на здравословни и безопасни условия на труд при работа с видеодисплеи (Издадена от министъра на труда и социалната политика и министъра на здравеопазването, обн., ДВ, бр. 70 от 26.08.2005 г.).

Чл. 25. Сървъри на локални компютърни мрежи /ако има такива/ се разполагат в самостоятелни помещения съобразно изискванията на Приложение № 11 към чл. 45 ал. 2 от Наредба за общите изисквания за оперативна съвместимост и информационна сигурност (Приета с ПМС № 279 от 17.11.2008 г).

Чл. 26. Всеки служител отговаря за целостта на компютърната и периферна техника, програмните продукти и данни, инсталирани на компютъра на неговото работно място или ползвани от него на сървъра на локалната компютърна мрежа съобразно дадените му права.

Чл. 27. Служителят има право да работи на служебен компютър, като достъпът до съхраняваните данни се осъществява от него с въвеждането на потребителско име и парола;

Чл. 28. Забранява се на външни лица работата с персоналните компютри на РДГ Благоевград, освен за упълномощени фирмени специалисти в случаите на първоначална инсталация на компютърна и периферна техника, програми, активни и пасивни компоненти на локални компютърни мрежи, комуникационни устройства и сервизна намеса на място, но задължително в присъствие на служител от РДГ Благоевград.

Чл. 29. След края на работния ден всеки служител задължително изключва компютъра, на който работи или го привежда в режим „log off“.

Чл. 30. При загуба на данни или информация от служебния компютър, служителят незабавно уведомява Системния администратор, който му оказва съответна техническа помощ;

Чл. 31. Забраняват се опити за достъп до компютърна информация и бази данни, до които не са предоставени права, съобразно заеманата от служителя длъжност, както и извършването на каквито и да е действия, които улесняват трети лица за несанкциониран достъп;

Чл. 32. Инсталиране и разместване на компютърни конфигурации и части от тях, на периферна техника, на активни и пасивни компоненти на локални компютърни мрежи, на комуникационни устройства се извършва само от системен администратор или съгласувано с него.

Чл. 33. Забранява се използването на преносими магнитни, оптични и други носители с възможност за презаписване на данни за прехвърляне на файлове между компютри, свързани в компютърната мрежа на РДГ Благоевград, освен с случаите, когато това е единствена възможност.

Чл. 34. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзка с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 35. Архивирана компютърна информация се предоставя само на служители, които имат право на достъп, съгласно заеманата от тях длъжност и изпълнявана задача, при спазване на принципа „необходимост да се знае."

Чл. 36. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, забрани за копиране, проследяване на несанкциониран достъп.

Чл. 37. Достъпът до помещенията, където са разположени сървърите /ако има

такива/ и комуникационните шкафове се ограничава по възможност само до специализиран по поддръжката им персонал.

РАЗДЕЛ VI
ПОЛЗВАНЕ НА КОМПЮТЪРНАТА МРЕЖА И ИНТЕРНЕТ

Чл. 38. Системният администратор извършва необходимите настройки за достъп до интернет, създава потребителски имена и пароли за работа с компютърната мрежа и електронната поща на РДГ Благоевград.

Чл. 39. Ползването на компютърната мрежа и електронната поща от служителите става чрез получените потребителско име и парола.

Чл. 40. Ползването на интернет и служебна електронна поща се ограничават съобразно скоростта на ползвания достъп до интернет, броя на откритите работни места и необходимостта от ползване на тези услуги съобразно служебните задължения на служителите.

Чл. 41. Служителите на съответните работни места са длъжни да не споделят своите потребителски имена и пароли с трети лица и носят дисциплинарна отговорност, ако се установи неправомерно ползване на ресурсите на компютърната мрежа, достъпа до интернет или електронна поща при използване на предоставените им потребителски имена и пароли.

Чл. 42. Компютрите, свързани в мрежата на РДГ Благоевград използват интернет само от доставчик, с когото има сключен договор за доставка на интернет.

Чл. 43. Забранява се свързването на компютри едновременно в мрежата на РДГ Благоевград и в други мрежи, когато това позволява разкриване и достъп до IP адреси от мрежата на РДГ и/или е в противоречие с изискванията на Закона за електронното управление (ЗЕУ) и НМИМИС за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.).

Чл. 44. Забранява се инсталирането и използването на комуникатори (като facebook, ICQ, Skype и др. подобни), осигуряващи достъп извън рамките на компютърната мрежа на РДГ Благоевград и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите, свързани в компютърната мрежа на РДГ Благоевград.

Чл. 45. Забранява се съхраняването на компютрите или сървърите на РДГ Благоевград на лични файлове с текст, изображения, видео и аудио.

Чл. 46. Забранява се отварянето без контрол от страна на системния администратор:

(1) получени по електронна поща или на преносими носители изпълними файлове, файлове с мобилен код и файлове, които могат да предизвикат промени в системната конфигурация, напр. файлове с разширения .exe, .vbs, .reg и архивни файлове;

(2) получени по електронна поща съобщения, които съдържат неразбираеми знаци

Чл. 47. Забранява се инсталирането и използването на неодобрен софтуер и фърмуер.

РАЗДЕЛ VII
ЗАЩИТА ОТ КОМПЮТЪРНИ ВИРУСИ И ДРУГ ЗЛОВРЕДЕН СОФТУЕР

Чл. 48. С цел антивирусна защита се прилагат следните мерки

(1) Всички персонални компютри имат инсталиран антивирусен софтуер в реално време, който се обновява ежедневно.

(2) Системният администратор извършва следните дейности:

2.1. активира защитата на съответните ресурси - файлова система, електронна поща и извършва първоначално пълно сканиране на системата;

2.2. настройва антивирусния софтуер за периодични сканирания през определен период, но поне веднъж седмично.

2.3. активира защитата на различните програмни продукти за предупреждение при наличие на макроси и настройва защитната стена на система;

2.4. проверява за правилно настроен софтуер за автоматично обновяване на

операционната система и инсталирания софтуер;

(3) При поява на съобщение от антивирусната програма за вирус в локалната мрежа, всеки служител от съответното работно място задължително информира Системния администратор.

РАЗДЕЛ VIII
НЕПРЕКЪСНАТОСТ НА РАБОТАТА

Чл. 49. Следните мерки се прилагат с цел антивирусна защита:

1. Всички сървъри /ако има такива/ и устройства за съхранение на данни да са свързани към устройство за непрекъсваемост на ел. снабдяването.
2. При липса на ел. захранване за повече от 10 мин., Системният администратор започва процедура по поетапно спиране на сървърите /ако има такива/.
4. При срив в локалната компютърна мрежа, всеки потребител следва да запише файловете, които е отворил на локалния си компютър, за да се избегне загуба на информация. При възстановяване на мрежата, всички локално запазени файлове следва да се преместят отново на сървъра /ако има такъв/.

РАЗДЕЛ IX
СЪЗДАВАНЕ НА РЕЗЕРВНИ КОПИЯ

Чл. 50. Системния администратор лице осигурява автоматизираното създаване на резервни копия на всички бази данни и електронни документи всеки ден.

Чл. 51 Информацията, включително тази, съдържаща лични данни, се архивира по следния начин:

(1) Автоматизирано и планово се извършва архивиране на цялата работна информация на сървърите /ако има такива/ и дисковите масиви.

(2) Архивирането на данните се извършва по начин, който позволява, при необходимост данните да бъдат инсталирани на друг сървър/ компютър и да се продължи работният процес без чувствителна загуба на данни;

(3) Базите данни на следните програми се архивират всяка вечер:

3.1. база данни на деловодна система „МИКСИ 2009“
3.2. база данни от програма „ТЕРЕЗ"
3.3. база данни от програма „КОНТО"

(4) Споделените документи се резервират 2 пъти седмично.

(5) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

(6) Съхраняват се най-малко последните три резервни копия.

(7) Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

Чл. 52. Всеки служител архивира създадената от него информация поне веднъж месечно в съответна директория на сървъра на РДГ.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в РДГ Благоевград са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от Директор и Зам. Директор и Системния администратор на РДГ.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността й, като РДГ Благоевград може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тези правила са разработени съгласно НМИМИС за минималните изисквания за мрежова и информационна сигурност (в сила от 26.07.2019 г.)

Изготвил:

Ваня Герчева - Системен администратор на РДГ Благоевград

Приложение № 1

АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

I. ВЪВЕДЕНИЕ

Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност.
По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

II. ОПРЕДЕЛЕНИЯ

Конфиденциалност - свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
Интегритет - качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
Наличност на информация - качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

III. ЦЕЛИ

1. Цел на процеса за управление на риска

Да минимизират загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях.

2. Цел на методиката за анализ и оценка на риска

Методиката има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от различните администрации, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:
2.1. регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2.2. определяне на критериите;
2.3. определяне на приоритетите на риска.

ПРЕПОРЪЧИТЕЛНА МЕТОДИКА

I. ЕТАПИ НА АНАЛИЗ И ОЦЕНКА НА РИСКА

Анализът и оценката на риска са част от процеса за управлението му и се обосновават на познаване на всички компоненти, имащи отношение към целите.
За целите на управлението на сигурността на мрежите и информационните системи трябва:
а) да се познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на НМИМИС (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация, поддържащите ги системи (електрозахранващи, климатизиращи и др.), оперативни процеси/дейности, служители и външни организации), наричани за краткост "информационни активи";
б) да се идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
в) да се оцени вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;

г) да се оцени въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
д) да се оцени рискът за сигурността;
е) да се набележат мерки за смекчаване на рисковете с висок приоритет.
При анализ и оценка на риска се използва регистър на рисковете (риск-регистър) (Примерен регистър на рисковете е даден в края на това приложение).

1. Идентифициране на информационните активи
В риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на тази наредба:
а) информационни системи;
б) хардуерни устройства, с които са реализирани информационните системи;
в) софтуери, с които са реализирани информационните системи;
г) бази данни, включително лични данни по смисъла на GDPR;
д) записи за събитията (логове, журнали) на информационните системи;
е) документация на информационните системи (експлоатационна и потребителска);
ж) комуникационни системи;
з) хардуерни устройства, с които са реализирани комуникационните системи;
и) фърмуерът на тези устройства;
к) софтуери на комуникационните системи;
л) записи за събитията (логове, журнали);
м) документация (експлоатационна и потребителска);
н) поддържащи системи (електрозахранващи, климатични);
о) системи за контрол на физическия достъп и на околната среда;
п) процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
р) документация на тези процеси и дейности;
с) служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
т) външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
у) друго.
2. Идентифициране на заплахите
За всеки от информационните активи в риск-регистъра се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.
Трябва да се разгледат всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.
(Примерни заплахи са посочени в края на това приложение).
В риск-регистъра за всяка заплаха се вписва какви мерки са предприети срещу нея.
3. Оценка на въздействието
В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие - щетите (материални и нематериални), които дадена заплаха може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.
4. Оценка на вероятността
Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:

а) за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;
б) за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.
В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.
За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:
1 - вероятността от реализирането на заплахата е под 10 %;
2 - вероятността от реализиране на заплахата е от 10 % до 30 %;
3 - вероятността от реализиране на заплахата е от 30 % до 50 %;
4 - вероятността от реализиране на заплахата е от 50 % до 70 %;
5 - вероятността от реализиране на заплахата е над 70 %.

5. Оценка на риска

За получаване на оценката на риска се използва следната формула:

(Оценка на въздействие x Оценка на вероятност) = Оценка на риска

6. Приоритизация на рисковете

С цел прилагане на пропорционални на заплахите механизми за защита се прави приоритизация на рисковете на база на тяхната оценка и следните прагове:

Приоритет на риска	Оценка на риска
1	от 17 до 25
2	от 8 до 17
3	от 1 до 8

7. Смекчаване на рисковете

Приема се, че за рискове с приоритет 3 не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.
За рисковете с приоритет 2 се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.
За всички рискове с приоритет 1 се определят отговорни лица, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

II. ПОСЛЕДВАЩИ ДЕЙСТВИЯ

Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплаха.

Ръководството на РДГ организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.

ПРЕПОРЪЧИТЕЛЕН РЕГИСТЪР НА РИСКОВЕТЕ

№ по ред	Информационен актив	Заплахи/ нежелани събития	Приложени мерки за защита	(от 1 до 5)Оценка на въздействието	Оценка на вероятността (от 1 до 5)	Оценка на риска	Приоритет на риска (от 1 до 3)	(за приоритет 3 и 2)рискаПланирани мерки за смекчаване на	Необходими ресурси	Отговорник за прилагане на планираните мерки	Срок за прилагане на планираните мерки

ВЕРОЯТНИ ЗАПЛАХИ

- Влошаване на средствата за съхраняване
- Грешка при техническото обслужване
- Грешки при предаването
- Електромагнитна радиация
- Зловреден програмен код
- Злоупотреба с ресурси
- Използване на неразрешени програми и данни
- Кражба
- Маскиране на потребителска идентификация (нелегално проникване)
- Неоторизиран достъп до компютри, данни, услуги и приложения
- Неоторизиран достъп до средствата за съхраняване
- Неправилна (погрешна) маршрутизация/пренасочване на съобщения
- Отричане (доказуемост)
- Повреда на комуникационното оборудване и услугите

- Подслушване
- Пожар, наводнение
- Потребителска грешка
- Администраторска грешка
- Прекъсване/повреда на захранването (електричество и климатизация)
- Претоварване на трафика
- Природни бедствия
- Кибератака
- Софтуерни проблеми
- Техническа повреда (мрежа, системен хардуер)