Врз основа на член 30 од Законот за класифицирани информации ("Службен весник на Република Македонија" број 09/2004), Владата на Република Македонија на седницата одржана на ден 7 март 2005 година, донесе

УРЕДБА

ЗА ИНФОРМАТИЧКА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Општи одредби

Член 1

Со оваа уредба се уредуваат мерките и активностите за информатичка безбедност за:

- сертификација на комуникациско-информатичките системи и процеси;
- процена за можно нарушување на безбедноста на комуникациско-информатичките системи;
- утврдување на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма;
- заштита на информациите при процесирање и чување во комуникациско-информатички системи;
- продукција на крипто клучеви и друг крипто материјал;
- криптографска заштита на комуникациски, информациски и други електронски системи преку кои се подготвуваат, пренесуваат, обработуваат и архивираат класифицирани информации;
- определување на зони и простории заштитени од компромитирачко електро-магнетно зрачење и
- инсталирање на уреди за чување на класифицирани информации.

Сертификација на комуникациско-информатички системи и процеси

Член 2

Државните органи и организациите (во понатамошниот текст: органите) кои планираат набавка или воспоставување на комуникациско-информатички систем за класифицирани информации до Дирекцијата за безбедност на класифицирани информации (во понатамошниот текст: Дирекција), доставуваат барање за безбедносна сертификација на комуникациско-информатичкиот систем (во понатамошниот текст: систем).

Член 3

Кон барањето од член 2 од оваа уредба се приложуваат следните документи:

- проценка на ризикот за безбедност на системот;
- изјава за безбедносни потреби на системот и
- процедури за безбедност при работа со системот.

Документите од став 1 на овој член се класифицираат со степен на класификација соодветен на највисокиот степен на класифицирани информации што се процесирааат со системот.

Член 4

Кога системот опфаќа повеќе органи, меѓу нив се склучува договор за поврзување на системите.

Договорот од став 1 на овој член се приложува кон барањето за сертификација на системот.

Член 5

Како последна фаза од процесот на сертификација на системот, се врши верификација на безбедноста на системот.

Член 6

Со верификација на безбедноста на системот се:

- потврдува дали соодветно се имплементирани планираните мерки за безбедност на системот, специфицирани во изјавата за безбедносни потреби;
- потврдува дека се имплементирани мерките за безбедност и дека е постигнато бараното ниво за безбедност преку соодветно тестирање;
- документираат резултатите од верификацијата на имплементацијата на безбедноста на системот, како податоци кои ќе се користат во текот на процесот на сертификација.

Член 7

По извршената проверка на системот се издава: сертификат за безбедност, сертификат за безбедност со ограничено траење или привремен сертификат за безбедност.

Член 8

За системите во кои се создаваат, обработуваат, чуваат или пренесуваат (во понатамошниот текст: процесираат) класифицирани информации со степен "Доверливо" и повисоко, се издава сертификат за безбедност на системот.

За системите во кои се процесираат информации класифицирани со степен "Интерно", кои согласно со Законот за класифицирани информации не подлежат на сертификација, се обезбедуваат услови за одржување на безбедносните цели (доверливост, интегритет и достапност) на информациите.

Проценка на можно нарушување на безбедноста на комуникациско-информатичките системи

Член 9

Проценка за можното нарушување на безбедноста на системот се врши за утврдување на ризикот, проценка на ризикот кој неможе да се избегне, оценка на повредливоста и заканите и утврдување на последиците од реализација на одредени закани.

Член 10

Проценка на ризикот и определување на соодветни мерки за заштита на системот се врши од страна на овластени лица на органот.

По потреба при проценка на ризикот може да се вклучат и надворешни стручни лица.

Член 11

Кога системот се користи во посебни услови (мобилни, теренски и други), при проценката на ризикот се оценуваат и ризиците поврзани со средината во која ќе се употребува системот.

Член 12

Проценка на повредливоста на системот се врши во временски рокови и со постапки за проценка на повредливоста на безбедноста на системот предвидени во планот за проценка на повредливоста на системот.

Утврдување на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицираните информации во електронска форма

Член 13

Локациите на системите во кои се процесираат класифицирани информации се определуваат како безбедносни и административни зони, согласно прописите за физичка безбедност на класифицираните информации.

Кога системот се користи во посебни услови (мобилни, теренски и други), се применуваат посебни услови за физичка безбедност.

Член 14

Во рамките на безбедносните зони се определуваат посебни простории за: електронска обработка на информациите, управување со системот, работа со криптографски средства и клучеви и архива на мемориски медиуми во кои се чуваат класифицирани информации.

Член 15

При определување на овластени лица за управување со безбедноста на системот се води грижа едно лице да не ги контролира сите важни елементи на безбедноста на системот.

Член 16

Системите во кои се процесираат класифицирани информации, треба да имат компјутерска безбедност особено за:

- идентификација на лицата кои пристапуваат во системот;
- контрола и евиденција на пристап до објектите на системот врз основа на дадено право за пристап од дефинирана база на податоци;
- континуиран запис на состојбата на системот, поврзано со безбедноста на системот (безбедносни записи), активноста на системот, измени на параметри и слично;
- можност за проучување на безбедносните записи и утврдување на активноста на корисниците поврзана со безбедноста на системот;
- поставување на програмски апликации во системот со кои ќе се оневозможи пристап на корисниците кои го изгубиле тоа право;
- обезбедување на сигурен начин за означување на степенот на класификација;
- идентификација на корисникот на отпечатениот, преснименият, модифицираниот или копираниот документ;
- сигурна евиденција на модифицирање, копирање, преснимување и бришење на класифицираните документи по корисници и
- заштита на важните технички и програмски елементи, системски можности и функционалност на системот.

Член 17

Системите во кои се процесираат класифицирани информации можат да работат во еден од следните степени:

- “Со посебно внимание”;

- “Високо ниво”;
- “Поделив пристап” и
- “Со повеќе нивоа”.

Член 18

Компјутерската безбедност на системите во режим на работа “Со посебно внимание”, “Високо ниво” и “Поделив пристап” се обезбедува со минималните барања за компјутерска безбедност.

Компјутерската безбедност на системите во степен на работа “Со повеќе нивоа” се реализира со безбедноста на системот согласно член 16 од оваа уредба и примена на дополнителна контрола за пристап на корисниците до програмските елементи на системот.

Заштита на информациите при процесирање и чување во комуникациско-информатичките системи

Член 19

Од страна на органите се контролираат и оценуваат сите промени во поширокатa, поблискатa и електронскатa средина за безбедност на системот и се преземаат мерки и постапки за безбедност и заштита на системот.

Член 20

За одржување на безбедноста и заштита на системот за време на неговото користење и развој се врши:

- повремена проверка на системите, средствата и преносните мемориски медиуми од аспект на квалитетот и исправноста;
- запишување на системските податоци и класифицираните информации во засебни надворешни мемориски медиуми и нивно чување на резервно место соодветно на највисокиот степен на класификација на снимените податоци;
- инсталирање на софтвер и конфигурирање на системот само од овластено лице;
- примена на нови технички и програмски средства во системот само по претходно добиен сертификат;
- сервисирање и поправка на средства од системот на начин кој не дозволува нарушување на безбедноста на системот и во согласност со условите од сертификацијата;
- замена на криптографски методи, средства и клучеви според одредбите на уредбата за криптозаштита или меѓународед договор;
- оценување и по потреба заштита од компромитирачко електромагнетно зрачење на средствата кои биле на сервис, поправка или ремонт и
- забрана за внесување и користење на компјутерски средства, медиуми за запис и софтвер во лична сопственост во безбедносните и административните зони на системот.

Член 21

Преносните комуникациско-информатички средства можат да се вклучат во сертифициран систем само ако се претходно сертифицирани за процесирање на информациите од соодветен степен на класификација и одобрени од страна на овластеното лице на органот.

Член 22

Класифицирани информации со степен “Државна тајна” и “Строго доверливо” не се процесираат во преносни комуникациско-информатички средства.

Член 23

Преносните мемориски медиуми во кои еднаш се зачувани класифицирани информации со степен "Државна тајна" и "Строго доверливо" се уништуваат по нивното декласифицирање.

Мемориските медиуми во кои се зачувани класифицирани информации со степен "Доверливо" и пониско, по нивната декласификација, можат да се задржат за натамошно користење.

Член 24

Амортизираните или оштетените мемориски медиуми во кои се зачувани класифицирани информации кои не може повеќе да се користат, се уништуваат.

Член 25

Во комуникациско-информатичките средства кои работат автоматски, без присуство на оператор, не се процесираат информации класифицирани со степен "Доверливо" и повисоко.

Член 26

Комуникациско-информатички средства и преносни мемориски медиуми (персонални компјутери, преносни компјутери, дискетни единици, мемориски елементи и слично) во лична сопственост не се користат за процесирање на информации класифицирани со степен "Интерно" и повисоко.

Член 27

Компјутерските преносни медиуми за запис на класифицирани информации кои се користат во системот се означуваат, регистрират и архивираат на начин кој соодвествува на медиумот во кој се сместуваат информациите.

Означувањето, контролата, архивирањето, периодичната контрола и уништувањето на компјутерските преносни медиуми за запис на класифицирани информации се врши според Уредбата за административна безбедност на класифицирани информации.

Член 28

Компјутерските преносни мемориски медиуми на кои се чуваат информаци и податоци кои обезбедуваат пристап до системот (посебни шифри, лозинки, елементи за идентификација) се заштитуваат со мерки соодветни на мерките за заштита на највисокиот степен на класифицирани информации во системот.

Информациите и податоците од став 1 на овој член, се уништуваат во согласност со процедурите за безбедност при работа со системот и на начин кој не дозволува обновување на мемориските запис.

Член 29

Преносните компјутерски средства и мемориски медиуми, кои се користат за процесирање на класифицирани информации, се сметаат како документи кои содржат класифицирани информации.

Изнесувањето на средствата од став 1 на овој член надвор од безбедносните зони се врши на ист начин како и другите класифицирани информации.

Продукција на крипто клучеви и друг крипто материјал

Член 30

Дистрибуцијата и чувањето на криптографските клучеви на системите за меѓународна размена на класифицирани информации се врши во рамките на Дирекцијата.

Дистрибуцијата и чувањето на криптографските средства и клучеви на системите за размена на класифицирани информации со странски држави и меѓународни организации се врши согласно со меѓународен договор.

Криптографска заштита на системите за класифицирани информации

Член 31

Пренос на класифицирани информации помеѓу централниот регистер и регистрите и контролните точки на Дирекцијата се врши преку обезбеден систем за криптозаштита.

Член 32

Со системите за криптозаштита на класифицирани информации се обезбедува:

- сигурна и заштитена идентификација на корисниците;
- потврда на автентичноста на испраќачот и примачот на информацијата кои треба да се извршат пред почнување на пренос на информацијата;
- доверливост, интегритет и достапност на информацијата и
- потврда за прием на информацијата.

Член 33

Класифицирани информациите не се пренесуваат преку комуникациски системи надвор од безбедносните зони без примена на криптографски методи и средства.

Член 34

Криптографски методи и средства за заштита на класифицирани информации со степен "Државна тајна" и "Строго доверливо" се користат и за заштита на информациите при нивното чување.

Определување на зони и простории заштитени од компромитирачко електромагнетно зрачење

Член 35

Системите кои се користат за процесирање на класифицирани информации со степен "Доверливо" и повисоко, се заштитуваат од компромитирачко електромагнетно зрачење.

Инсталирање на уреди за чување на класифицирани информации.

Член 36

Класифицираните информации се чуваат во уреди, инсталирани од стручни и овластени лица на органите.

Завршна одредба

Член 37

Оваа уредба влегува во сила осмиот ден од денот на објавувањето во "Службен весник на Република Македонија".

Бр._____
_____ 2005
Скопје

Председател
на Владата на Република Македонија
д-р Владо Бучковски, с.р.