FOUNDATION ФОНДАЦИЈА
OPEN ИНСТИТУТ
SOCIETY ОТВОРЕНО
INSTITUTE ОПШТЕСТВО
MACEDONIA МАКЕДОНИЈА

Подобрување на имплементацијата и примената на Законот за слободен пристап до информации од јавен карактер, на Законот за безбедност на клацифицирани информации и на Законот за заштита на личните податоци

2

Дирекција за безбедност на класифицирани информации

Лидија Костовска, в.д.директор

Скопје, 30 мај 2007

ЗАКОНСКА РАМКА ЗА ИНФОРМАТИЧКА БЕЗБЕДНОСТ

2004 г. - Закон за класифицирани информации

- Уредба за административна безбедност на класифицирани информации

- Уредба за физичка безбедност на класифицирани информации

- Уредба за безбедност на лица корисници на класифицирани информации

2005 г. - Уредба за информатичка безбедност на класифицирани информации

- Уредба за индустриска безбедност на класифицирани информации

ЗАКОНСКА РАМКА ЗА ИНФОРМАТИЧКА БЕЗБЕДНОСТ- продолжува

Меѓународни прописи:

-НАТО безбедносна политика Ц-М(2002)49 и 50 и директиви во состав

-Primary Directive on INFOSEC AC/35-D/2004, AC/322-D/0052

-INFOSEC Management Directive AC/35-D/2005

-Бројни упатства, инструкции и прегледи на НАТО (повеќе од 20-тина)

ИНФОРМАТИЧКА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

- Заштита на информациите што се создаваат, се чуваат или се пренесуваат во комуникациски, во информатички или во други електронски системи од случајно или намерно губење на тајноста, интегритетот или достапноста и
- Превенција од губење на интегритетот и достапноста на системите во коишто се создаваат, се чуваат или низ коишто се пренесуваат информациите;
- Примена на комбинирани безбедносни мерки за создавање безбедно опкружување за работа на комуникациски, на информатички и на други електронски системи

МЕРКИ ЗА ИНФОРМАТИЧКА БЕЗБЕДНОСТ НА ИНФОРМАЦИИ

- Информатичката безбедност ги опфаќа мерките за компјутерска безбедност (COMPUSEC), комуникациска безбедност (COMSEC) и емисиона безбедност (TEMPEST), и тоа:

- Процена на безбедносен ризик
- Дефинирање на безбедносни потреби
- Криптографска заштита на КИС
- Темпест зони и средства
- Инсталирање електронски средства и опрема
- Безбедносни оперативни процедури и
- Безбедносна акредитација на КИС

ОРГАНИЗАЦИЈА НА УПРАВУВАЊЕТО СО КИС

Управувањето со комуникациско-информатички системи се организира преку определување авторитети на повеќе нивоа, и тоа:

- **Авторитет за безбедносна акредитација** (Одделение за безб.акредитација во ДБКИ)
- **Авторитет за планирање и имплементација** (оддел, сектор или одделение за КИС во органот/институцијата)
- **Оперативен авторитет** (лице одговорно за оперативна работа на КИС)
- **Овластено лице за безб.на клас.информации** (лице овластено од органот/институцијата)
- **Администратор на безбедноста на КИС** (овластено лице за безбедност на КИС)
- **Корисници на КИС** (корисници кои имаат дозвола за работа со КИС)

ПРОЦЕНА И УПРАВУВАЊЕ СО БЕЗБЕДНОСЕН РИЗИК НА КИС

- **Закани за безбедноста на комуникациско-информатичките системи (разузнавачки служби,терористички оргнизации, вандали, хакери, криминални активности, медиуми за информации, политички екстремисти, незадоволен персонал, погрешно обучени корисници)**
- **Слабости на комуникациско-информатичките системи(да се направи детално техничко испитување на безбедносните елементи и способности на КИС-евалуација; да се издаде потврда дека КИС ги задоволува безбедносните барања врз основа на прегледот на резултатите од евалуацијата-сертификацијата и да се изврши одобрување на КИС за работа со класифицирани информации-акредитација)**

ПРОЦЕНА И УПРАВУВАЊЕ СО БЕЗБЕДНОСЕН РИЗИК НА КИС- продолжение

- **Процена на безбедносен ризик (поддршка од раководниот тим во органот/институцијата, да се избере квалификуван тим за процена, да се разбере целта и широчината на проценатa и да се даде преглед и одобрување на извештајот за проценатa; проценатa содржи попис на физички средства и информации, во неа се определува нивната важност, се идентификуваат заканите и ранливоста, се идентификуваат безбедносните мерки)**
- **Управување со безбедносен ризик (во проценатa на безбедносниот ризик се дефинира прифаќањето на истиот преку прифаќање на предложените безбедносни мерки и активности и се изработува извештај за управување со ризикот на КИС)**

ЕМИСИОНА БЕЗБЕДНОСТ НА КИС

Комуникациско-информатичките системи за информации класифицирани со степен „Доверливо” и повисоко се заштитуваат со мерки и активности за противемисиона заштита на начин со којшто:

- се набавува ТЕМПЕСТ опрема (видео монитори, компјутери, принтери, скенери, факсови, фотокопири, телефони, модеми и кабелски инсталации и конектори;

- се врши зонирање на просториите (Зона 0-минимално слабеење, Зона 1-мало слабеење; Зона 2-средно слабеење, Зона 3-максимално слабеењена емисијата);

- се инсталира КИС во согласност со одобреното упатство.

ПОДОБРУВАЊЕ НА ИМПЛЕМЕНТАЦИЈАТА НА ЗКИ ОД АСПЕКТ НА ИНФОБЕЗ

- **Изработка на Национална програма за информатички развој во Република Македонија**
- **Комуникација, соработка и координација меѓу државните органи и институции по однос на динамиката на спроведувањето на Националната програма за информатички развој**
- **Експертска помош од странски земји и меѓународни организации и институции во имплементацијата на Програмата**
- **Преземање мерки и активности за контрола врз спроведувањето на безбедносните стандарди и процедури (ДБКИ-консултации, соработка, координација, контрола)**

ПОДОБРУВАЊЕ НА ПРИМЕНАТА НА ЗКИ

- **Обука на сите лица кои ги контролираат и работат со КИС за правилна примена на ЗКИ, подзаконските акти и другите меѓународни прописи**

- **Кревање на нивото на информатичкото образование и безбедносната култура во Република Македонија**