

АСПЕКТИ НА ЗАЩИТАТА НА СЛУЖЕБНАТА ИНФОРМАЦИЯ

инж. Чавдар Пенков
АКИС

СЪДЪРЖАНИЕ

1. Какво е информация?
2. Защо е необходимо да я защитаваме;
3. Определение на информационна сигурност на една КИС;
4. Нормативна база;
5. Подзаконови актове;
6. Изисквания към КИС и сигурността на информацията;
7. Заплахи към сигурността на информацията;
8. Решения за защита на информацията в КИС;

КАКВО Е ИНФОРМАЦИЯ?

ИНФОРМАЦИЯТА Е ФИЛОСОФСКО ПОНЯТИЕ, ОТРАЗЯВАЩО ПОЗНАНИЕТО ВЪВ
ВСЯКА ОБЛАСТ НА ЖИВОТА, ИЗРАЗЕНО ЧРЕЗ СЪОТВЕТНИ ХАРАКТЕРНИ ЗНАЦИ.

В СЪВРЕМЕННИЯТ СВЯТ ВСЯКО ПОЗНАНИЕ СЕ ИЗРАЗЯВА ЧРЕЗ ИНФОРМАЦИЯ.

ЗА ДА РАЗВИВАМЕ НАШИТЕ ДЕЙНОСТИ, Е НЕОБХОДИМО ДА **ОБМЕНЯМЕ** РАЗЛИЧНИ
ИНФОРМАЦИИ ПО **КАНАЛИТЕ НА КОМУНИКАЦИОННИТЕ МРЕЖИ**. СЪВРЕМЕННИТЕ
МРЕЖИ ПОЗВОЛЯВАТ ТАЗИ ИНФОРМАЦИЯ ДА СЕ ПРЕДАВА НА ГОЛЕМИ РАЗСТОЯНИЯ,
МЕЖДУ ОТДАЛЕЧЕНИ КОРЕСПОНДЕНТИ.

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

ЗАЩО Е НЕОБХОДИМО ДА СЕ ЗАЩИТАВА ИНФОРМАЦИЯТА?

В МНОГО ОТ ЧОВЕШКИТЕ ОТНОШЕНИЯ СЕ ОБМЕНЯ **ЧУВСТВИТЕЛНА
ИНФОРМАЦИЯ**, КОЯТО Е НЕОБХОДИМО НАДЕЖДНО ДА СЕ ЗАЩИТИ ОТ ЧУЖДИ
ПОГЛЕДИ. ТАЗИ ИНФОРМАЦИЯ МОЖЕ ДА Е:

- **КЛАСИФИЦИРАНА – ДЪРЖАВНА ИЛИ СЛУЖЕБНА ТАЙНА**, ОТРАЗЯВАЩА
ДЕЙНОСТИ ПО СИГУРНОСТТА НА ДЪРЖАВАТА ИЛИ ВЗАИМООТНОШЕНИЯ В
НАДНАЦИОНАЛНИ ОРГАНИЗАЦИИ И СЪЮЗИ, ИЛИ
- **НЕКЛАСИФИЦИРАНА СЛУЖЕБНА** – КАСАЕЩА РАЗЛИЧНИ СЛУЖЕБНИ ДЕЙНОСТИ В
ДАДЕНА ОРГАНИЗАЦИЯ, КОИТО Е ЖЕЛАТЕЛНО ДА НЕ СЕ РАЗПРОСТРАНЯВАТ БЕЗ
САНКЦИЯ НА РЪКОВОДСТВОТО Й.

ЗА ПОЛЗВАЩИТЕ **ИНФОРМАЦИЯ** Е НЕОБХОДИМО ДА СЕ ОСИГУРИ
ЛЕСЕН ДОСТЪП ДО НЕЯ – **НАЛИЧНОСТ**,
ДА НЕ СЕ ПРОМЕНЯ СЪДЪРЖАНИЕТО Й ПРИ ПРЕНАСЯНЕ – **ЦЯЛОСТНОСТ**,
В МНОГО СЛУЧАИ НЕ ТРЯБВА ДА СЕ ВИЖДА ОТ ЧУЖДИ ОЧИ - **КОНФИДЕНЦИАЛНОСТ**.

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

ИНФОРМАЦИОННОТО ОСИГУРЯВАНЕ ЗА ЕДНА КОМУНИКАЦИОННО-ИНФОРМАЦИОННА СИСТЕМА (КИС)

*„Информационното осигуряване е **съвкупност от мерки за сигурност** за достигане на необходимото ниво на конфиденциалност по отношение сигурността и защитата на информацията в комуникационно-информационната система (КИС), както и на самата КИС, чрез осигуряване **конфиденциалност, интегритет, наличност, гарантиране на афтенитичност на информацията и невъзможност тя да бъде отказана, при дейности изпълнявани през тази КИС.**“*

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

НОРМАТИВНА БАЗА

ИНФОРМАЦИЯ	НАЦИОНАЛНА	НАТО	ЕС
ДЪРЖАВНА ИЛИ СЛУЖЕБНА ТАЙНА	ЗАКОН ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ (ДЪРЖАВЕН ВЕСТНИК, бр. 45 ОТ 30.04.2002 г.) И ПОДЗАКОНОВИТЕ НОРМАТИВНИ АКТОВЕ	ДИРЕКТИВА ЗА СИГУРНОСТТА В НАТО С-М(2002)47 ЗА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ В АЛИАНСА	SECURITY REGULATION (редакция 2009 г.) на СЪВЕТА НА ЕВРОПА ЗА ЕВРОПЕЙСКА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ
МАРКИРОВКА	СТРОГО СЕКРЕТНО СЕКРЕТНО ПОВЕРИТЕЛНО ЗА СЛУЖЕБНО ПОЛЗВАНЕ	COSMIC TOP SECRET NATO SECRET NATO CONFIDENTIAL NATO RESTRICTED	EU TOP SECRET EU SECRET EU CONFIDENTIAL EU RESTRICTED

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

НОРМАТИВНА БАЗА

ИНФОРМАЦИЯ	НАЦИОНАЛНА	НАТО	ЕС
НЕКЛАСИФИЦИРАНА СЛУЖЕБНА	ВСЕ ОЩЕ НЕ Е ПРИЕТА НОРМАТИВНА УРЕДБА	ДИРЕКТИВА ЗА УПРАВЛЕНИЕ НА НЕКЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ НА НАТО С-М(2002)60	ОЧАКВА СЕ РАЗРАБОТВАНЕТО НА ОТДЕЛЕН ДОКУМЕНТ
МАРКИРОВКА	-	NATO UNCLASSIFIED	EU LIMITE

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

ОБХВАТ НА НОРМАТИВНАТА БАЗА

ПОДЗАКОНОВАТА РЕГУЛАТОРНА РАМКА ОБХВАЩА ВСИЧКИ
ЕЛЕМЕНТИ ОТ КОМПЛЕКСА МЕРКИ ЗА ОСИГУРЯВАНЕ
СИГУРНОСТТА НА ИНФОРМАЦИЯТА:

1. ПЕРСОНАЛНА СИГУРНОСТ;
2. ДОКУМЕНТАЛНА СИГУРНОСТ;
3. ФИЗИЧЕСКА СИГУРНОСТ;
4. КРИПТОГРАФСКА СИГУРНОСТ;
5. СИГУРНОСТ НА АИС / МРЕЖИ;

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

ОСГУРЯВАНЕ НА ИНФОРМАЦИЯТА В КОМУНИКАЦИОННО-ИНФОРМАЦИОННИТЕ СИСТЕМИ ВКЛЮЧВА:

1. ИЗГРАЖДАНЕ НА ФИЗИЧЕСКА И ДОКУМЕНТАЛНА СИГУРНОСТ НА МЕСТАТА ЗА РАЗПОЛАГАНЕ ЕЛЕМЕНТИТЕ НА КИС;
2. ИЗГРАЖДАНЕ НА КИС С ОДОБРЕН ХАРДУЕР И СОФТУЕР;
3. ДОСТИГАНЕ НА НЕОБХОДИМА ПЕРСОНАЛНА СИГУРНОСТ ЗА ОБСЛУЖВАЩИ (АДМИНИСТРАТОРИ) И ПОЛЗВАТЕЛИ НА КИС;
4. ВЪВЕЖДАНЕ И ПОДДЪРЖАНЕ НА ПОЛИТИКИ ЗА СИГУРНОСТ ПРИ ПОЛЗВАНЕ НА КИС;
5. ОЦЕНКА НА ЗАПЛАХИ И РИСКОВИ ФАКТОРИ И СЪЗДАВАНЕ ОРГАНИЗАЦИЯ ЗА ПРЕОДОЛЯВАНЕТО ИМ И НЕПРЕКЪСВАЕМА РАБОТА;
6. КОМУНИКАЦИОННАТА СИГУРНОСТ;

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

ЗАПЛАХИ КЪМ ИНФОРМАЦИЯТА

ВЪНШНИ:

ПОДСЛУШВАНЕ - ПРИХВАЩАНЕ И ИЗВЛИЧАНЕ НА ИНФОРМАЦИЯТА;

ИЗМЕНЕНИЕ - УМИШЛЕНА ПРОМЯНА НА ЧАСТ ОТ ИНФОРМАЦИЯТА;

ПОДПРАВЯНЕ - ИЗПРАЩАНЕ НА СЪОБЩЕНИЕ ОТ ИМЕТО НА ПОЗНАТ ЗА ПОЛУЧАТЕЛЯ АДРЕСАТ;

ВЪНШНИ ЗАВИСИМОСТИ - ВОДЕЩИ ДО НЕВЪЗМОЖНОСТ ДА СЕ ПОЛУЧИ СЪОБЩЕНИЕТО.

ВЪТРЕШНИ

НЕДОБРОСЪВЕСТНИ СЛУЖИТЕЛИ - УМИШЛЕНА ПРОМЯНА НА ИНФОРМАЦИЯТА;

НЕРАЗРЕШЕН ДОСТЪП - ИЗВЛИЧАНЕ И ПОЛЗВАНЕ НА ИНФОРМАЦИЯТА В УЩЪРБ НА ОРГАНИЗАЦИЯТА ;

ЧОВЕШКИ ГРЕШКИ - НЕУМИШЛЕНА ПРОМЯНА НА ИНФОРМАЦИЯТА;

НЕЯСНИ РЕШЕНИЯ - ВОДЕЩИ ДО СЪСТАВЯНЕ НА ГРЕШНИ ИНФОРМАЦИИ;

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

РЕШЕНИЯ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

Решенията трябва да бъдат **комплексни**:

- Да изпълняват изискванията на действащата нормативна уредба **при изграждане на сигурни комуникационно-информационни системи**;
- Да осигуряват на администраторите на изградени КИС **инструменти за своевременно откриване и предприемане на адекватни мерки за предотвратяване на уязвимостите и заплахите**;
- Да изградят гъвкава и надеждна **криптографска защита на информацията** за постигане на елемента конфиденциалност при преноса ѝ през общо достъпните комуникационни среди.

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

РЕШЕНИЯ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

Без криптография

- Изграждане на мрежи за служебна информация без класификация с прилагане на мерки за автентификация и идентификация на външните ползватели;
- Изграждане на вътрешно ведомствени мрежи със собствени физически защитени комуникационни канали – използвана се за мрежи, работещи в ограничени контролируеми райони;

С Off-Line Криптография

- Предварителна криптографска обработка на информацията, прилагана в контролируема защитена среда, с криптографски пособия, отговарящи на съответното ниво на КИ.

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)

РЕШЕНИЯ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА

On-Line Криптография

- Изграждане на вътрешно ведомствени мрежи с криптографска защита на комуникационните канали – използва се за мрежи, пренасящи високо ниво на КИ и работещи в ограничени контролируеми райони;
- Изграждане на виртуални защитени канали през общо достъпната комуникационна среда за отделни части на мрежовата система, изградени по изискванията на нормативната база – използва се за мрежи със средно и ниско ниво на класификация на информацията, както и за мрежи със служебна неклассифицирана информация;
- Изграждане на индивидуална криптографска защита от високо ниво за отделен IP адрес.

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)



ВЪПРОСИ

инж. ЧАВДАР ПЕНКОВ,
Член УС на АКИС

Mobile: +359(888)561 487
E-mail: penkov@itagroup.bg

[АСОЦИАЦИЯ НА КОМУНИКАЦИОННО ИНФОРМАЦИОННИТЕ СПЕЦИАЛИСТИ](#)