Безопасность информации электронного правительства

КАЛИН КАЛИНОВ,
ЭКСПЕРТ МИНИСТЕРСТВА ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ БОЛГАРИЯ

3-я Международная конференция
"Россия – Балканы: доверие и безопасность в информационном обществе“
12-16 сентября 2011 года,
Черногория, г. Херцег-Нови

Государственная политика в области информационной безопасности

ЗАКОН ОБ ЭЛЕКТРОННОМ ДОКУМЕНТЕ И ЭЛЕКТРОННОЙ ПОДПИСИ – 2002 Г.
ЗАКОН О ЗАЩИТЕ ЛИЧНЫХ ДАННЫХ – 2002 Г.
ЗАКОН ОБ ЭЛЕКТРОННЫХ КОММУНИКАЦИЯХ – 2007 Г.
ЗАКОН ОБ ЭЛЕКТРОННОМ УПРАВЛЕНИИ – 2007 Г.

ШЕСТЬ ПОЛОЖЕНИЙ К ЗАКОНУ ОБ ЭЛЕКТРОННОМ УПРАВЛЕНИИ, В Т.Ч.:
- ОБ ОПЕРАТИВНОЙ СОВМЕСТИМОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ;
ОБ ЕДИНОЙ СРЕДЕ ОБМЕНА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ;
ОБ ЭЛЕКТРОННЫХ АДМИНИСТРАТИВНЫХ УСЛУГАХ И ПР.

Безопасность информации электронного правительства

В отличии от преобладающей до сих пор практики автономного развития информационных систем в каждой администрации, требования Закона об однократном вводе данных о гражданах и фирмах вызывает интенсивный обмен между административными системами. Это создает новые типы угроз безопасности, такие как:

- перенос уязвимостей от одной системы к другой;

- блокирование електронных административных услуг одной системы при нарушенной доступности другой и пр.

Поэтому, достижение определенного приемлемого уровня информационной безопасности всех систем становится обязательным условием их взаимодействия.

Это требование усугубляется участием в разработке пан-Европейских транс-граничных электронных административных услуг.

Безопасность информации электронного правительства

Государственная политика в области информационной безопасности сформулирована в “Положении об основных требованиях к оперативной совместимости и информационной безопасности” к Закону об электронном управлении, принятой Советом министров в ноябре 2008-ого года.

Основами для ее разработки являются:

1. Международные стандарты:

- ISO/IEC 270XX (information security management systems);

- ISO / IEC 15408-2 (Common Criteria);

- рекомендации Международного союза телекоммуникаций (ITU) X.800 и X.805

2. Коммюнике Европейской комиссии COM (2006) 251

3. Руководство ITU по национальной самооценке в области кибер-безопасности

4. Результаты проекта IBM-България “Security Architecture”, относящегося к ре-инженерингу болгарской централной администрации

5. Рекомендации и методологические руководства Европейского агентства сетевой и информационной безопасности (ENISA)

Безопасность информации электронного правительства

1.Центральный уровень включает в себя следующие меры:

1.1. Централизованное управление Государственной телекоммуникационной сетью под методологическим контролем МТИТС;

1.2. Создание Правительственного центра реагирования при компьютерных инцидентах (Gov-CERT);

1.3. Создание Единой среды гарантированного обмена электронных документов (ЕСОЭД);

1.4. Внедрение Национальной структуры административных метаданных;

1.5. Проведение унифицированной политики развития Disaster Recovery Centers;

1.6. Организация Центрального органа контроля за информационной безопасностью в администрации в составе МТИТС

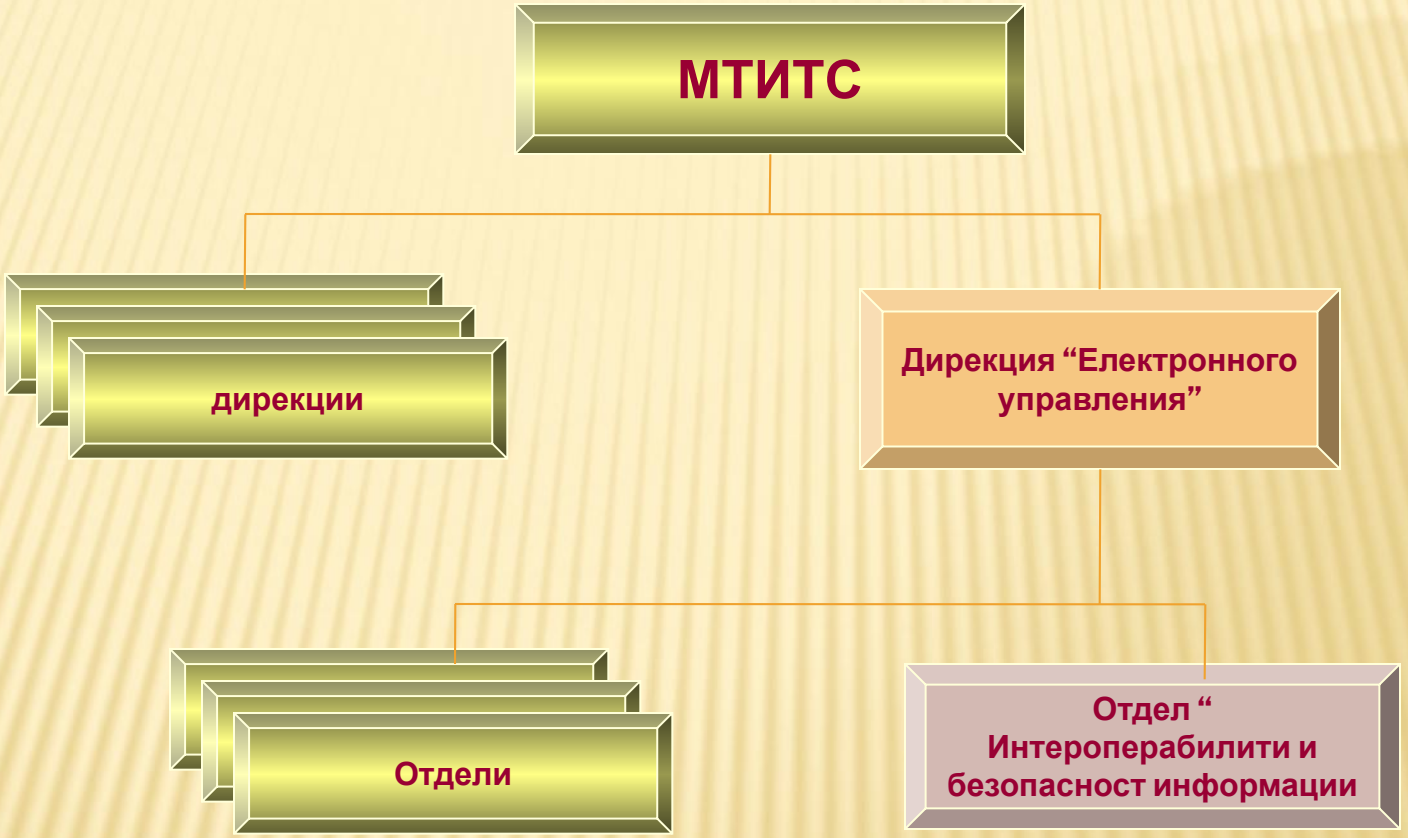
Безопасность информации электронного правительства

2. Уровень административного органа базируется на:

2.1. Создании “Системы управления информационной безопасностью”, регламентированной стандартом ISO 27001:2005;

2.2. Специфической сертификации административных информационных систем в соответствии с Положением об оперативной совместимости и информационной безопасности к Закону об электронном управлении

Безопасность информации электронного правительства



Безопасность информации электронного правительства

Отдел «Интероперабильности и информационной безопасности”

- разработку и обновление политики и программ по информационной безопасности и совместимости информационных систем;
- разработку и применение норм и стандартов , регистров для интероперабильности и информационной безопасности в соответствии с Законом электронного управления и его правил, а также регистры экспертов, аккредитованных и сертифицированных систем и продуктов;
- определение требований к совместимости и информационной безопасности и соблюдение контроля;
- подготовку позиций, анализа и информации по вопросам взаимодействия и информационной безопасности.

Безопасность информации электронного правительства

Структура защиты инфраструктуры электронного правительства состоит из мер и процедур, основанных на требованиях Правил общих требований интероперабильности и информационной безопасности Закона электронного управления.

К ним относятся:

- Организационные меры
- Технические меры

Безопасность информации электронного правительства

Реализованные средства управления доступом участников в электронном обмене включают в себя три категории функций:

а) административные функции;
б) вспомогательные;
в) информационные функции.

Безопасность информации электронного правительства

Руководители администрации обеспечивают необходимую физическую защиту информационных систем путем реализации следующих мер:

а) управление мерами физического доступа;
б) меры противопожарной защиты;
с) защиты содержающей инфраструктуры ;
г) защиты мобильных систем.

БЛАГОДАРЮ ЗА ВНИМАНИЮ!