Обеспечение доверия при идентификации и аутентификации пользователей электронных госуслуг и дальнейшем использовании их учетных данных

Елена Онишко
Консультант в области международного сотрудничества и развития глобального информационного общества. Член МАС

Региональный семинар МСЭ для стран СНГ

"Развитие электронного правительства как одно из условий интеграции в глобальное информационное общество "

г. Москва, Российская Федерация, 25-27 ноября 2013 года

План презентации

- Методы идентификации и аутентификации
- *[Технические и программные средства идентификации и аутентификации]*
- *[Провайдеры услуг по идентификации и аутентификации]*
- Административные процедуры и организационные меры обеспечения доступа к учетным данным
- Использование учетных данных
- *Аналитическая обработка учетных данных*
- Риски несанкционированного доступа к учетным данным
- Административное регулирование
- *Правовое регулирование*
- Формирование электронного правительства в России
- Международный опыт
- Вопросы доверия при использовании электронных госуслуг
- Открытые вопросы

i. Идентификация и аутентификация

Идентификация -
именование и опознавание;

Аутентификация -
подтверждение подлинности пользователей системы

Получение государственных услуг

1. Методы идентификации и аутентификации

Аутентификация пользователей

- Программно-аппаратная аутентификация при доступе к сети (MAC, Web, 802.1X)
- Парольная аутентификация;
- Предмет с уникальным содержимым или с уникальными характеристиками;
- Аутентификационная информация - неотъемлемая часть пользователя;
- Аутентификация посредством GPS

Аутентификация данных

- ЭЦП

Административные процедуры и меры доступа к учетным данным

- **Единая система идентификации и аутентификации** (ЕСИА) — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах.

Сценарий идентификации и аутентификации в ЕСИА

1. Пользователь обращается к защищённому ресурсу информационной системы (например, ведомственному или региональному порталу государственных услуг).
2. Информационная система направляет в ЕСИА запрос на аутентификацию.
3. ЕСИА проверяет наличие у пользователя открытой сессии и, если активная сессия отсутствует, проводит его аутентификацию. Для этого ЕСИА направляет пользователя на веб-страницу аутентификации ЕСИА. Заявитель проходит идентификацию и аутентификацию, используя доступный ему метод аутентификации.
4. Если пользователь успешно аутентифицирован, то ЕСИА передаёт в информационную систему набор утверждений, содержащих идентификационные данные пользователя, информацию о контексте аутентификации, в том числе данные об уровне достоверности идентификации.
5. На основании полученной из ЕСИА информации, информационная система авторизует заявителя на доступ к защищаемому ресурсу.

Выдержки из портала госуслуг

- Информационная безопасность является одной из важных компонент предоставления государственных услуг в электронном виде. При создании ЕПГУ проводилась работа по анализу возможных угроз, на основе которых сформированы требования по защите информации при использовании портала госуслуг. В системе безопасности портала госуслуг используется обширный набор механизмов безопасности: межсетевые экраны, средства анализа содержимого, средства предотвращения вторжений, антивирусные средства, средства мониторинга и контроля защищенности.

  Программное обеспечение портала госуслуг проходит сертификацию по требованиям информационной безопасности и отсутствию недекларированных возможностей.

  Единый портал госуслуг аттестован по требованиям ФСТЭК на обработку конфиденциальной информации и персональных данных по требованиям класса К1.

  Для доступа на портал используется система аутентификации на основе электронной подписи, реализованная с помощью решений, прошедших сертификацию в ФСБ.

  При этом необходимо помнить, что безопасность определяется не только уровнем защиты портала, но и уровнем защиты рабочего места, с которого осуществляется доступ. В частности, для нормальной работы с порталом госуслуг пользователь должен следовать следующим рекомендациям:
- - Использовать на рабочем месте исключительно лицензионное программное обеспечение;
- - Устанавливать все необходимые обновления безопасности, рекомендуемые производителем программного обеспечения:
- - Устанавливать и регулярно обновлять антивирусное программное обеспечение, регулярно проводить проверку на отсутствие вирусов;
- - Не загружать программ и данных из непроверенных источников, не посещать сайты сомнительного содержания;
- - Не заходить в личный кабинет портала госуслуг со случайных компьютеров, интернет-кафе либо иных недоверенных рабочих мест;
- - Не передавать кому-либо токены для авторизации на портале, либо информацию для входа в личный кабинет, следить за сохранностью средств доступа.

  Если уровень защиты персонального компьютера вызывает сомнения, более безопасным способом является заказ услуг при помощи инфомата.

Административные процедуры и меры доступа к учетным данным

Основные документы, определяющие стандарты аутентификации:

- ГОСТ Р ИСО/МЭК 9594-8-98 - Основы аутентификации
- FIPS 113 - COMPUTER DATA AUTHENTICATION
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 - Выбор защитных мер

Использование учетных данных и доверие в цифровом обществе (ii)

- 1) Доверие между людьми в обществе, которое позволяет всесторонне использовать цифровые технологии для общения и проведения сделок;
- 2) Доверие (или уверенность) людей в инфраструктуре цифровых сетей и систем, которыми они пользуются для оказания/получения услуг, общения, хранения данных, вычислений и пр.

Использование учетных данных и доверие в цифровом обществе (i)

Препятствия для доверия в онлайн-среде:

- Отсутствие идентификаторов
- Отсутствие личных характеристик
- Неопредленные обстоятельства

Административное регулирование

- Концепция информационной политики,1998
  - построение информационного общества
- Концепция программы «Развитие информатизации в России»
  - программа создания условий для перехода страны к информационному обществу
- Окинавская хартия глобального информационного общества, 2000
  - распространение ИКТ и преодоление информационного неравенства
- Административная реформа
  - 2004-2006 – первый этап
  - 2006-2010 – второй этап – продолжение и коррекция

Административное регулирование – направления деятельности (I)

Изменение идеологии, философии и технологий управления (административная реформа)

- проактивный подход к потребностям граждан
- возросшая роль граждан
- пересмотр функций органов публичной власти
- сокращение бюрократических издержек
- проектный подход к управлению

Изменение организационной структуры и внедрение новых управленческих технологий

- национальный план развития электронного правительства
- государственные услуги
- создание национальной ИКТ-инфраструктуры электронного правительства
- обучение информационным технологиям и ликвидация компьютерной безграмотности

Административное регулирование – направления деятельности (II)

3. Изменение нормативно-правовой базы в сфере телекоммуникаций и развития Интернет

4. Информационная политика государства в контексте электронного правительства

5. Структура управления электронным правительством

6. Доверие граждан, коммерческого сектора к деятельности государства, в целом, и в вопросах электронного правительства, в частности.

Риски несанкционированного доступа к учетным данным

- Уязвимость парольной аутентификации (простота пароля, легкость его перехвата, фишинг и т.п.)

Проблемы формирования электронного правительства в России

- Низкая распространенность информационных технологий в стране
- Распад СССР - глубокие структурные изменения политической системы
- Масштабность
- Проблема бюрократии второстепенна

Формирование электронного правительства в России

- Доступ к информации о деятельности органов власти
  - первый шаг по информированию населения о деятельности власти

  Результат – повышение прозрачности деятельности федеральных органов государственной власти, и также региональных органов, с помощью ИКТ

- ФЦП «Электронная Россия (2002-2010) №2»
  - программа формирования электронного правительства в Российской Федерации

- Взаимодействие федерального центра с регионами
  - отсутствие четкой политики центра в области информатизации
  - недостаток финансирования региональных проектов электронного правительства
  - недостаточная разработанность законодательной базы

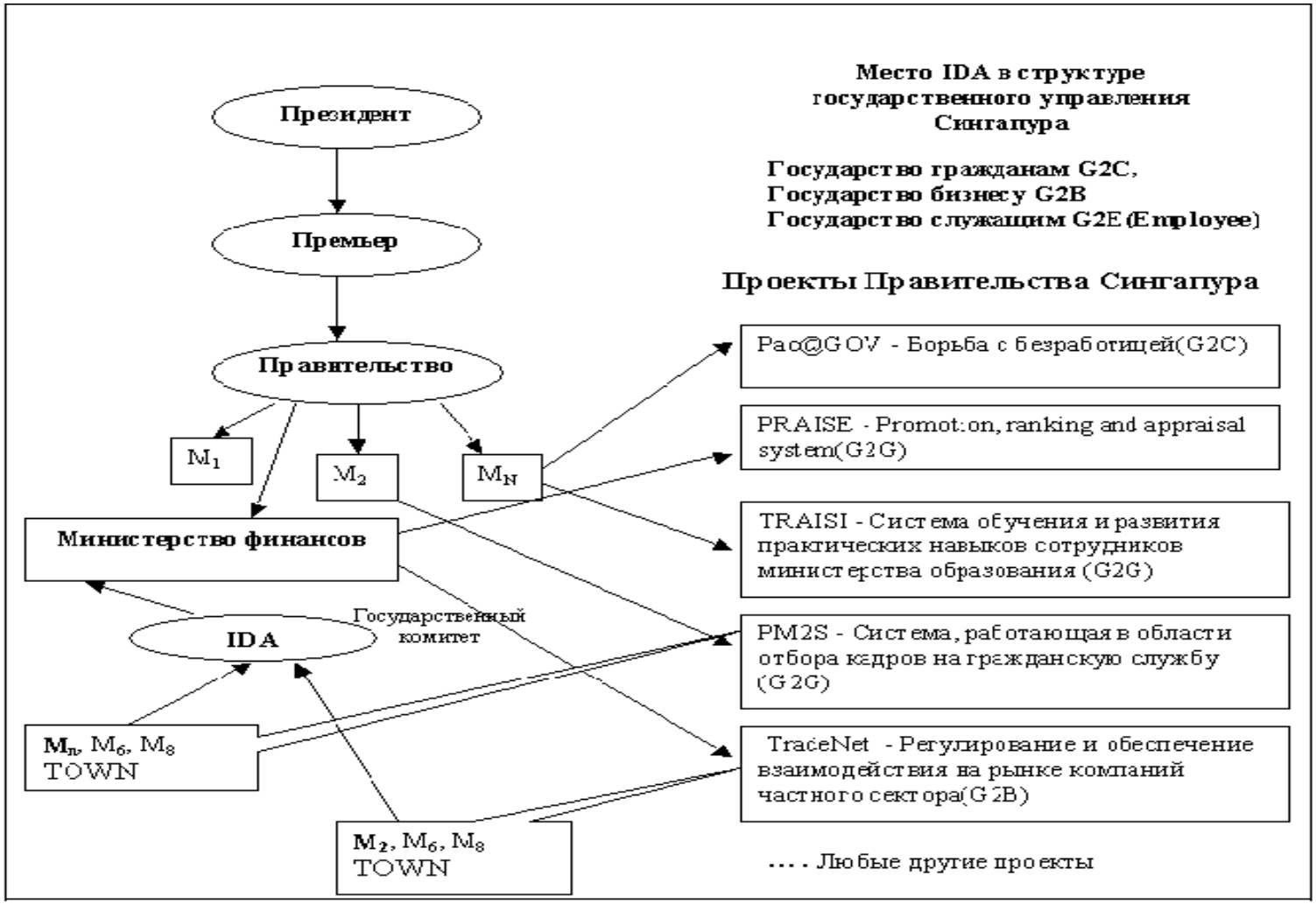
  2007-2008 гг. – первые типовые программно-технические решения, направленные на использование ИКТ на региональном уровне

Международный опыт

Международный опыт. Национальная система электронного правительства - Сингапур (I)

- Государственное агентство IDA (Infocommunication Development Agency), 1999 г.
- Создание «городов» (TOWN)
- Стратегические планы государства
- Государственная комиссия по стандартизации
- Закон об электронных транзакциях, 1998 г.
- Защищенная телекоммуникационная сеть (Интранет), государственный портал, до 2000 г.
- Национальный портал «E-citizen» (электронный гражданин) и система государственных закупок GeBiz

Структура государственного управления Сингапура (ЭП)



Международный опыт. Национальная система электронного правительства - США (II)

- 90-х годы XX века - системный подход к развитию электронного правительства

Законы:

о безбумажном документообороте и свободе информации, 1995 г.

о реформе использования информационных технологий, закон Клинджера–Коэна, 1996 г.

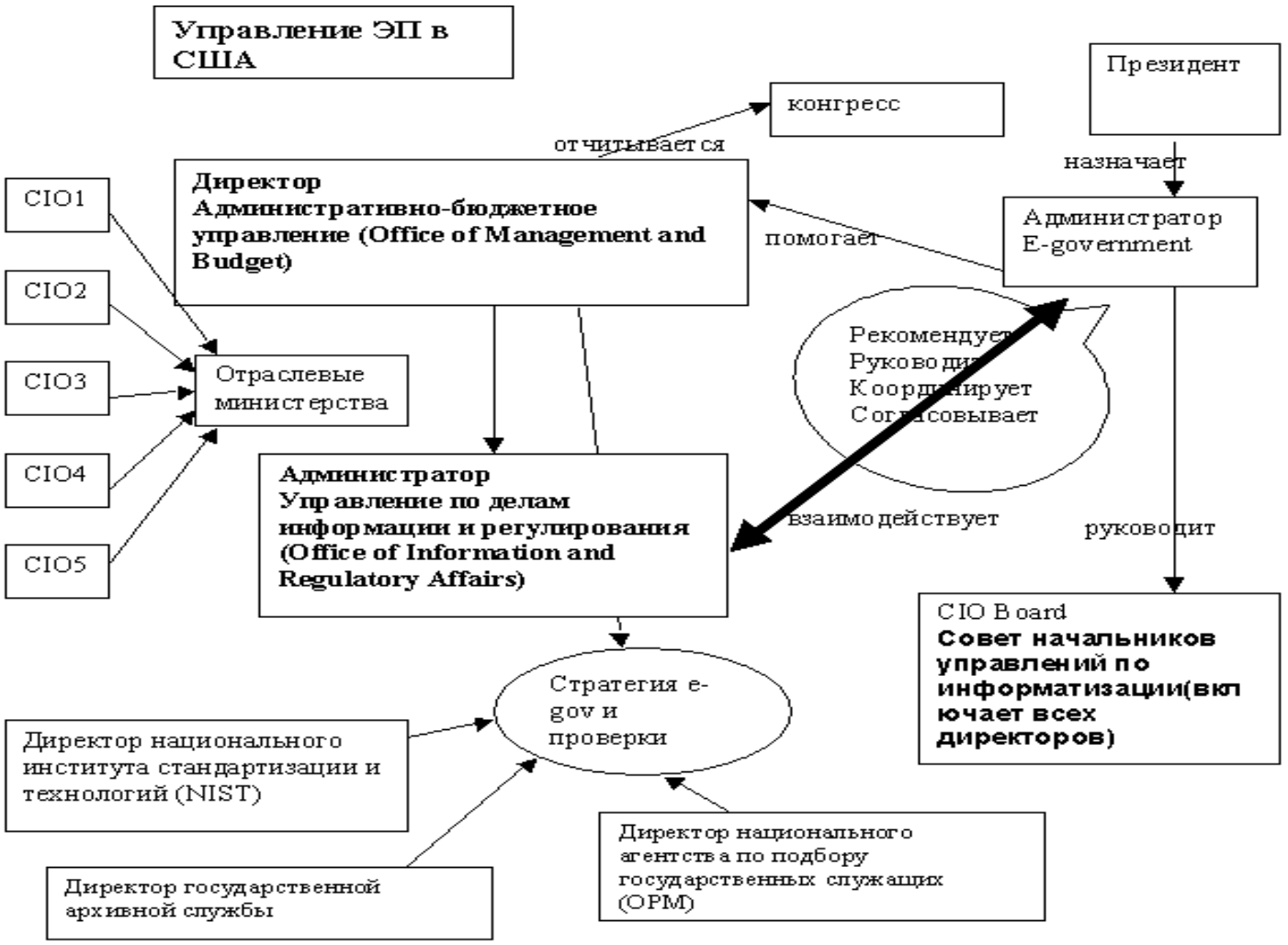
о свободе информации, 1996 г.

- Инвестирование в ИТ-инфраструктуру
- 11 сентября 2001 – изменение государственной политики – борьба с терроризмом

Patriot Act, 2001

- Управление по делам информации и регулирования (Office of Information and Regulatory Affairs)
- Совет ИТ-директоров отраслевых федеральных Министерств (CIO)
- Гибкость законов о государственной службе

Структура государственного управления США (ЭП)



Открытые вопросы

СПАСИБО!

- Ваши вопросы