ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ

при удаленном электронном взаимодействии

А.Сабанов, зам. генерального директора ЗАО "Аладдин Р.Д.", к.т.н.

В статье рассматриваются некоторые актуальные проблемы идентификации при удаленном электронном взаимодействии. Автор показывает, что эта область информационного взаимодействия нуждается в регулировании.

Введение

Развитие государственной программы "Информационное общество (2011–2020 годы)" [1] выявило необходимость надежной идентификации сторон удаленного электронного взаимодействия. Анализ нормативной базы [2] показал, что методика идентификации граждан, обращающихся за государственными и муниципальными услугами, пока практически осталась вне области регулирования. Этот пробел в нормативной базе может приводить как к злоупотреблениям правами граждан (например, незаконное получение материнского капитала), так и к прямым злоумышленным действиям от имени ничего не подозревающего гражданина (например, передача прав его собственности). В связи с этим актуально исследование теоретических основ надежности идентификации субъектов. В работе [3] рассмотрены основные методы повышения надежности сложных информационных систем. Показано, что для анализа надежности систем идентификации и аутентификации (СИА) необходимо выполнить подробное описание системы, идентифицировать риски, выявить опасные события, провести анализ последствий и их частоты, сформулировать критерии отказа и надежности выполнения системой заданных функций. Пример идентификации рисков типового процесса аутентификации рассмотрен в работе[4].

Определения

Согласно руководящему документу [5], идентификатором называется уникальный признак субъекта или объекта доступа. В качестве идентификаторов граждан может использоваться номер паспорта, СНИЛС, ИНН.

Идентификация – это сравнение идентификатора, который вводит участник информационного взаимодействия в любую из информационных систем, указанных в пункте 4 Требований [6], с идентификатором этого участника, который содержится в базовом государственном информационном ресурсе, определяемом Правительством Российской Федерации.

Системы и способы идентификации

Рассмотрим наиболее распространенные способы идентификации на примере хорошо изученных систем управления доступом. Можно выделить три независимых группы свойств идентификаторов.

К первой группе отнесем свойства идентификаторов как характеристик принадлежности (собственности): универсальный (У), формируемый и выдаваемый на федеральном уровне, и корпоративный (К).

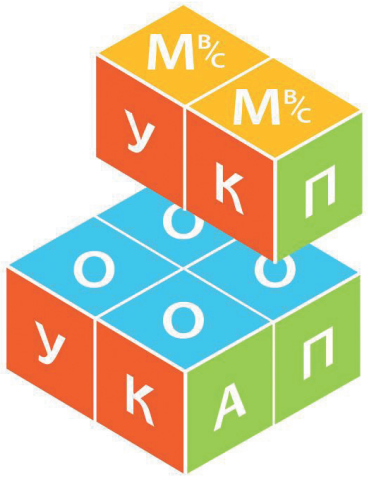
Ко второй группе отнесем свойство идентификаторов распознавать личность владельца: анонимный (А) или персональный (П).

Третья группа свойств идентификаторов характеризует доступ владельца к ресурсам: одноразовый (О) или многоразовый (М).

Нетрудно догадаться, что число возможных комбинаций равно $2^3 = 8$, однако в жизни реализуется всего шесть комбинаций, изображенных на рисунке.

В ряде случаев для повышения достоверности идентификации необходимо добавить еще один идентификатор – биометрическую характеристику владельца. Этот тип идентификатора – расширение первой группы свойств идентификаторов: к универсальному и корпоративному добавляется личный (Л). Анализ показывает, что в физическом и виртуальном мире из 12 возможных реализуется всего семь комбинаций: к шести изображенным на рисунке добавляется кубик с гранями ЛПМ – личный, персональный, многоразовый.

Предложенный подход позволяет систематизировать способы идентификации.



Комбинации свойств распространенных идентификаторов

Ошибки идентификации

Вероятность ошибки идентификации можно оценить с помощью соотношения:

$$P = \prod_{i=1}^{k} p_i,$$

где p_i – вероятность ошибки идентификации по i-му идентификатору, k – число идентификаторов.

Приведем пример идентификации личности по двум представленным документам (идентификаторам).

Предположим, что вероятность ошибки идентификации по первому идентификатору составляет 10^{-4}, по второму – 10^{-6}. Тогда вероятность ошибки идентификации составит $P = 10^{-10}$. С учетом того, что население Российской Федерации оценивается в 140 млн. человек, т.е. $1{,}4 \cdot 10^8$, вероятная суммарная ошибка идентификации составит 1,4%. Однако эти примитивные оценки справедливы при условии так называемых доверенных источников и процессов идентификации.

При недостаточной степени достоверности идентификации по выбранным параметрам необходимо вводить дополнительные идентификационные признаки, а в приведенную формулу добавлять поправочные коэффициенты. Для проведения практических оценок этот процесс проще всего свести к рассмотрению вероятностных интервалов ожидаемых значений для всех (в том числе добавленных) p_i. Например, в условиях недостаточной достоверности в рассмотренном примере вероятность ошибки по первому идентификатору может оцениваться в пределах 10^{-4}–10^{-3} или в более широких пределах в зависимости от степени доверенности. Тогда суммарная ошибка может быть оценена как граница произведений наибольших значений p_i. Математически можно добиться желаемой (или заданной) точности идентификации введением одного или нескольких дополнительных идентификаторов даже в условиях недостаточной достоверности по каждому из рассматриваемых признаков.

На практике желательно в качестве идентификационных признаков вводить идентификаторы, зарегистрированные в различных ведомственных базах данных (например, ФМС, ФНС, ПФР). Для снижения рисков злоупотреблений также рекомендуется введение хотя бы одного неотчуждаемого от пользователя (например, биометрического) идентификатора. По логике общественной безопасности база данных биометрической идентификации граждан должна находиться в ведении МВД России.

В теории идентификации рассматривают ошибки первого и второго рода.

Ошибка первого рода состоит в том, что в результате проведенной идентификации пользователя не идентифицировали как легального зарегистрированного пользователя в системе. Это может случиться, например, при наличии "двойника" или из-за сбоя в работе системы. В терминах теории надежности такое событие может трактоваться как отказ системы идентификации.

Ошибка второго рода применительно к задаче идентификации может быть сформулирована как идентификация злоумышленника под видом легального пользователя системы. Применительно к задаче оценки надежности системы такое событие называется опасным отказом.

Оценки вероятности наступления отказа системы и опасного отказа лучше проводить для конкретной системы с заданными характеристиками. Для промышленных систем, как правило, вероятность наступления опасного отказа как минимум на порядок меньше вероятности наступления отказа системы. Это обстоятельство необходимо учитывать при проектировании систем идентификации.

Применение сертификата ключа проверки квалифицированной электронной подписи для идентификации субъектов

Один из развивающихся способов идентификации сторон удаленного электронного взаимодействия – идентификация субъекта по его сертификату ключа проверки подписи (СКПП). Субъект получает свой СКПП по запросу в центре регистрации (ЦР) удостоверяющего центра (УЦ). На УЦ возлагается всего четыре основные задачи:

- установление личности заявителя – будущего владельца СКПП;
- формирование по установленному алгоритму цифрового сертификата проверки подписи и заверение его электронной подписью УЦ;
- выдача СКПП под личную собственноручную подпись его владельцу;
- поддержка выданного сертификата в течение всего срока его действия.

Из выданных СКПП значительную часть составляют сертификаты должностных лиц предприятий и организаций. Заполненные без ошибок поля СКПП в абсолютном большинстве случаев позволяют однозначно идентифицировать юридическое лицо, в котором работает владелец сертификата. При этом, однако, для идентификации субъекта – владельца СКПП заполняются всего три поля: ФИО, электронный адрес в произвольном формате и СНИЛС. Фактически ФИО пригодны для идентификации субъекта лишь относительно (вспомним число однофамильцев в крупных организациях), а единственный уникальный идентификатор – СНИЛС.

Поскольку СКПП – это своего рода аналог электронного паспорта, первая из перечисленных задач УЦ (установление личности заявителя) становится одной из важнейших. Однако на текущий момент, несмотря на наличие ряда методических указаний по заполнению полей сертификата, процесс установления личности не регламентирован. ЦР, действуя от лица УЦ, не протоколирует этапы представления заявителем идентификаторов и результаты

их проверок и не хранит эти записи в своем защищенном архиве. Заметим, что в развитых странах ЦР обязан выполнять эти элементарные требования для разбора конфликтных ситуаций. Например, в США указанные требования к ЦР регулируются стандартом [7], обязательным к исполнению.

К сожалению, при выдаче СКПП физическим лицам дело с идентификацией владельца сертификата обстоит не лучше. Правила аккредитования УЦ (на сегодня при Минкомсвязи аккредитовано 338 УЦ) позволяют выдавать СКПП в удаленном режиме. Имеются УЦ, в рекламе которых говорится о выдаче СКПП за 15 минут в режиме удаленного электронного взаимодействия. Какое доверие может быть к СКПП, выданным этим способом? Очевидно, вопросы идентификации участников электронного взаимодействия по СКПП нуждаются в срочном регулировании.

ЛИТЕРАТУРА

1. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. №1815-р "О государственной программе Российской Федерации "Информационное общество (2011–2020 годы)".
2. **Сабанов А.Г.** Обзор иностранной нормативной базы по идентификации и аутентификации. – Инсайд. Защита информации, 2013, №4 (52), с.82–88.
3. **Сабанов А.Г.** Методы исследования надежности удаленной аутентификации. – Электросвязь, 2012, №10, с.20–24.
4. **Сабанов А.Г.** Методика идентификации рисков процессов аутентификации. – Доклады Томского государственного университета систем управления и радиоэлектроники, 2013, №4 (30), с.136–141.
5. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: Гостехкомиссия России, 1992.
6. Постановление Правительства РФ от 28 ноября 2011 г. №977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".
7. FIPS PUB 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2011. http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf, 01.11.2013.