УДК 004.089

А.Г. Сабанов

О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии

Рассмотрена задача исследования достоверности идентификации пользователя при удаленном электронном взаимодействии. Разработана методика определения ошибок идентификации. Показана необходимость использования биометрических методов идентификации для снижения уровня ошибок идентификации. Обоснована задача доработки нормативной базы в части регулирования идентификации пользователя при удаленном электронном взаимодействии.
Ключевые слова: идентификация, достоверность, проблема, пользователь, удаленное электронное взаимодействие.

Вопросы идентификации сторон при удаленном электронном взаимодействии (УЭВ) в связи с развитием информатизации общества [1] занимают одно из первых мест по актуальности. К числу особенно сложных и до сих пор не до конца решенных проблем безопасности относится надежная идентификация субъектов и объектов при УЭВ. Действительно, в целях противодействия нарастающему мошенничеству весьма важно знать, какой именно субъект находится на другой стороне сеанса взаимодействия. Несмотря на обилие западных нормативных документов, регулирующих процессы идентификации и аутентификации, рассмотренных в работе [2], вопросы достоверности идентификации до конца не решены. Под достоверностью идентификации будем понимать общую точность и полноту идентификационной информации об объекте. Достоверность идентификации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Схема идентификации должна быть удобной для применения пользователями и простой для организации онлайн-сервисов. Общие вопросы идентификации и аутентификации рассмотрены в работе [3], однако вопросы достоверности идентификации не вошли в данное исследование. В работе [4] изучены общие методы анализа надежности применительно к процессам аутентификации, которые были применены к задаче идентификации рисков в работе [5]. Одним из выводов перечисленных работ явилось установление факта отсутствия типовых схем, математических моделей и подходов к анализу надежности и достоверности идентификации при УЭВ. Мало того, как показано в работе [1], отечественная нормативная база по вопросам идентификации субъектов при УЭВ и доступе к онлайн-сервисам нуждается в серьезной доработке. Целью данной работы является разработка модели и методики оценки достоверности идентификации пользователя при УЭВ.

Модель исследования электронной идентификации. Формализуем процесс идентификации. Существующие системы идентификации (СИ), как правило, используют последовательные запросы на соответствие предъявленного субъектом идентификатора Id_i с занесенным ранее в базу данных. Типовая схема идентификации представлена на рис. 1.

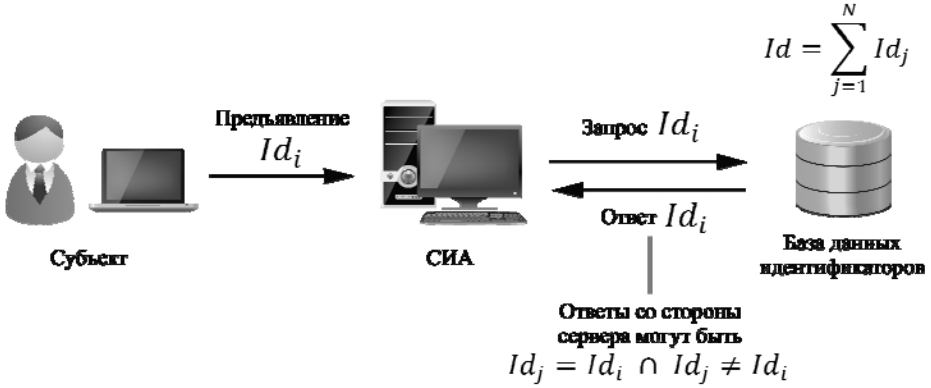

Рис. 1. Типовая схема идентификации субъекта

Предъявленный субъектом идентификатор принимается системой идентификации и аутентификации (СИА), которая высылает автоматический запрос в базу данных идентификаторов. Если предъявленный идентификатор Id_i совпадает с находящимся в базе Id_j, т.е. $Id_i = Id_j$, то идентифика-

ция считается пройденной успешно. В агрессивной к атакам среде сравниваться могут не сами значения Id_i, а их свертки (хеши). Современные СИА могут быть настроены на использование не одного, а нескольких идентификаторов – избыточность числа идентификаторов делается с целью повышения надежности процесса идентификации. Рассмотрим СИ – подсистему СИА, отвечающую только за процесс идентификации.

Модель процесса идентификации представлена на рис. 2.

Рис. 2. Модель предъявления идентификаторов субъектом, число идентификаторов $n = 3$

Количество идентификаторов в процессе их предъявления взаимодействующей стороне (чаще всего это информационной ресурс – сервер) может быть $n = 1, 2, 3$. Случаи $n > 3$ на практике встречаются весьма нечасто, однако покажем, что предлагаемые в данной работе подходы легко могут быть распространены на любое n. Предположим, что в базе данных находится N зарегистрированных идентификаторов: $Id = \sum_{j=1}^{N} Id_j$.

Ответы со стороны сервера могут быть $Id_j = Id_i \cap Id_j \neq Id_i$, где Id_i – предъявленный субъектом идентификатор.

В такой системе критерием успешной идентификации будет совпадение не одного, а заданного числа n предъявленных идентификаторов. Рассмотрим эту типовую модель процесса последовательного предъявления и проверки идентификаторов с точки зрения теории надежности информационных систем.

Согласно основным положениям теории структурной надежности [6] сначала определим условия работоспособности системы и сформулируем критерии отказа. Предполагается, что элементы (в рассматриваемом случае c_i – процедуры идентификации по Id_i, $i = 1, 2, 3$) отказывают независимо друг от друга, т.е. отказ любых элементов не изменяет надежности остальных элементов.

Пусть E будет событием элемента c_i, происходящего в определенный момент времени. Безотказность СИ для представленной на рис. 2 модели может быть представлена в виде

$$P_C = \prod_{i=1}^{n} P[E_i].$$

В случае известных распределений наработок до отказа отдельных элементов $F_i(t) = 1 - P_i(t)$ для независимых элементов вероятность безотказной работы СИ определяется выражением

$$P_C(t) = \prod_{i=1}^{n} [1 - F_i(t)] = \prod_{i=1}^{n} P_i(t) .$$

Принятым в большинстве работ по надежности подобных систем функцией распределения отказов в каждом элементе $F_i(t)$ является экспоненциальное распределение наработки до отказа

$$F_i(t) = 1 - P_i(t) = 1 - e^{-\lambda_i t}$$

с постоянной интенсивностью отказов $\lambda_i = \text{const}$, $i = 1, 2, 3$. Обозначим $\Lambda = \sum_{i=1}^{n} \lambda_i$. Тогда

$$P_C(t) = \exp(-\sum_{i=1}^{n} \lambda_i t) = \exp(-\Lambda t) .$$

При условии $\Lambda t \ll 1$ допустимы следующие приближенные выражения: $P_C(t) \approx 1 - \Lambda t$ и $Q(t) \approx \Lambda t$, где $Q(t) = 1 - P_C(t)$ – вероятность отказа.

Другими словами, вероятность безотказной работы системы идентификации в данном случае всегда меньше, чем вероятность отсутствия отказов самого ненадежного элемента. Она существенно возрастает при увеличении надежности самого ненадежного элемента.

При этом априори должны выполняться 2 условия:

- «доверенный» источник (база данных идентификаторов);
- «доверенные» процедуры идентификации.

На практике оба условия выполняются не в полной мере, лишь с какой-то долей вероятности.

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, в результате наличия «двойника» и/или сбоя при сравнении отдельного идентификационного параметра (параметров), превышения заданного уровня ошибок и сбоев в работе самой 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 определим как опасный отказ.

Оценки вероятности наступления отказа и опасного отказа лучше проводить для конкретной системы с заданными характеристиками. При этом можно воспользоваться математическими моделями надежности, разработанными в работе [7].

Приведем пример идентификации субъекта взаимодействия по двум представленным документам (идентификаторам). Предположим, что вероятность ошибки идентификации по первому идентификатору составляет 10^{-4}, по второму – 10^{-6}. Тогда суммарная вероятность ошибки идентификации составит $P = 10^{-10}$. С учетом того, что население Российской Федерации оценивается в 140 млн человек, т.е. $1{,}4\times10^{8}$, 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 идентификации по каждому из рассматриваемых идентификационных 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. При этом эта база данных нуждается в современной системе управления доступом и должна быть обеспечена высокотехнологичным средством защиты конфиденциальности данных, например представленным в работе [8, 9].

Применение сертификата ключа проверки квалифицированной электронной подписи для идентификации субъектов. Одним из развивающихся способов идентификации сторон удаленного электронного взаимодействия является идентификация субъекта по его сертификату ключа проверки подписи (СКПП). Субъект получает свой СКПП по запросу в центре регистрации (ЦР) удостоверяющего центра (УЦ). На УЦ возлагаются следующие основные задачи:

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

Остановимся на первой задаче, которая на момент написания статьи фактически не регулируется. Из выданных на сегодня СКПП значительную часть представляют собой сертификаты должностных лиц предприятий и организаций. Заполненные без ошибок заданные поля СКПП (O, S, C, STREET, OID = 1.2.643.3.131.1.1 и 1.2.643.100.1) в абсолютном большинстве случаев позволяют однозначно идентифицировать юридическое лицо, в котором работает владелец сертификата. При этом, однако, для идентификации субъекта – владельца СКПП заполняются всего 3 поля: CN (ФИО), E (электронный адрес в произвольном формате), СНИЛС. Фактически для идентификации субъекта относительно пригодны только ФИО (вспомним число полных однофамильцев в крупных организациях) и СНИЛС, который является единственным уникальным идентификатором.

Поскольку СКПП является своего рода аналогом электронного паспорта, первая из перечисленных задач УЦ (установление личности заявителя) является 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.

К сожалению, при выдаче СКПП физическим лицам дело с идентификацией владельца сертификата обстоит не лучше. Правила аккредитования УЦ (на момент написания данной статьи при Минкомсвязи России аккредитовано 317 УЦ) позволяют выдавать СКПП в удаленном режиме. Имеются УЦ, в рекламе которых говорится о выдаче СКПП за 15 мин в режиме удаленного электронного взаимодействия. Вопросы доверия к СКПП, выданным таким способом, остаются без ответа.

Заключение. Разработанная методика позволяет проводить оценки достоверности идентификации пользователя при УЭВ. Установлено, что вопросы идентификации участников электронного взаимодействия, в том числе по СКПП, нуждаются в дальнейшем исследовании и регулировании. Возможно, одним из путей решения проблемы станет принятие федерального закона об идентификации и аутентификации пользователей информационных систем. Однако обсуждение и принятие законов обычно длится достаточно долгое время. Независимо от появления такого закона Минкомсвязи России необходимо сформулировать и установить правила регистрации новых пользователей ИС и владельцев СКПП.

Литература

1. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)». [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html, свободный (дата обращения: 17.12.2013).

2. Сабанов А.Г. Обзор иностранной нормативной базы по идентификации и аутентификации // Инсайд. Защита информации. – 2013. – № 4 (52). – С. 82–88.

3. Аутентификация. Теория и практика / Под ред. А.А. Шелупанова. – М.: Горячая линия – Телеком, 2009. – 552 с.

4. Сабанов А.Г. Методы исследования надежности удаленной аутентификации // Электросвязь. – 2012. – № 10. – С. 20–24.

5. Сабанов А.Г. Методика идентификации рисков процессов аутентификации // Доклады ТУСУРа. – 2013. – № 4 (30). – С. 136–141.

6. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. – Ульяновск: Печатный двор, 2012. – 216 с.

7. Сабанов А.Г. Концепция моделирования процессов аутентификации // Доклады ТУСУРа. – 2013. – № 3(29). – С. 71–75.

8. Додохов А.Л. К вопросу о защите персональных данных с использованием СУБД Oracle / А.Л. Додохов, А.Г. Сабанов // Доклады ТУСУРа. – 2012. – № 2 (26). – С. 129–133.

9. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2–1. – С. 61–67.

Сабанов Алексей Геннадьевич
Канд. техн. наук, зам. генерального директора ЗАО «Аладдин Р.Д.», доцент МГТУ им. Н.Э. Баумана
Тел.: 8-985-924-52-09
Эл. почта: asabanov@mail.ru; a.sabanov@aladdin-rd.ru

Sabanov A.G.

On problem of user identification reliability for remote electronic interaction

The problem of reliability examination of user identification in remote electronic interaction is considered. An identification errors detection technique is developed. The necessity of use of biometric identification methods for lowering identification errors rate is shown. The task of modification of regulatory framework for user identification in remote electronic interaction is justified.

Keywords: identification, reliability, problem, user, remote electronic interaction.