УРОВНИ ДОВЕРИЯ К РЕЗУЛЬТАТАМ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Сабанов А.Г.[1]

Цель статьи: *разработка концепции формирования уровней доверия к результатам идентификации и аутентификации граждан при переходе к цифровой экономике.*

Метод*: синтез концепции на основе анализа международных стандартов, процессов идентификации и аутентификации, а также оценки рисков ошибок идентификации и аутентификации в задачах управления доступом к информационным ресурсам и системам.*

Полученный результат*: Выполнен анализ международных и ряда национальных стандартов, касающихся доверия к идентификации и аутентификации. Проанализированы процессы идентификации и аутентификации, а также участники процессов. На основе выполненного анализа и оценки рисков сформулированы критерии доверия к результатам идентификации и аутентификации. Показано, что доверие к идентификации субъекта доступа определяется качеством выполнения первичной идентификации гражданина, то есть достоверностью определения того, является ли субъект тем, за кого себя выдает. Разработаны методы оценки доверия к результатам первичной идентификации.*

Установлено, что доверие к результатам аутентификации определяется достигнутым доверием к первичной идентификации субъекта доступа при регистрации, доверием к обеспечению конфиденциальности секрета (аутентифицирующей информации) на протяжении всего его жизненного цикла, а также доверием к корректности реализации методов аутентификации, включающих в себя организацию обмена аутентификационной информации между заявителем и сервером аутентификации (односторонний или взаимный обмен), используемые при этом факторы аутентификации и протоколы обмена. Предложен метод оценки доверия к результатам аутентификации зарегистрированного субъекта доступа в пространстве безразмерных параметров, разработанный в соответствии с предложенными критериями доверия. На основе выполненного анализа разработана концепция формирования уровней доверия к результатам идентификации и аутентификации, отличающаяся от известных зарубежных аналогов учетом специфики применения сертифицированных средств криптографической защиты информации и средств аутентификации.

Ключевые слова: *первичная идентификация, оценка рисков, аутентифицирующая информация, метод аутентификации, уровень доверия, критерии доверия, субъект доступа.*

DOI:10.21681/2311-3456-2019-5-19-25

В связи с интенсивным развитием государственной программы «Цифровая экономика» вопросы предоставления безопасного доступа граждан к информационным ресурсам различного назначения становятся весьма актуальными. Управление доступом включает в себя сервисы идентификации и аутентификации (ИА), предназначенные для определения подлинности пользователя [1]. Сервис идентификации включает в себя первичную идентификацию (ПИ), проводимую в каждой информационной системе (ИС) однократно во время регистрации нового пользователя, и вторичную идентификацию, с помощью которой система идентификации и аутентификации (СИА) каждой ИС при любом запросе на доступ отфильтровывает «своих» (зарегистрированных) пользователей от случайных и зачастую нежелательных гостей [2]. Если этот фильтр пройден (то есть предъявленный идентификатор нашелся среди имеющихся в данной ИС), зарегистрированный в данной системе пользователь должен пройти процедуру аутентификации, подтвердив подлинность предъявленного идентификатора и его принадлежность данному субъекту доступа с помощью предъявления аутентификационной информации (АИ). Целью аутентификации является формирование необходимой уверенности в том, что субъект доступа действительно является тем зарегистрированным субъектом (объектом) доступа, за кого себя выдает [3]. Для большинства государственных организаций и коммерческих компаний весьма важным является вопрос о том, насколько система управления доступом и особенно процессы ИА способны преградить доступ к информационным ресурсам нежелательным субъектам, но предоставлять доступ легальным пользователям с заданным уровнем доверия [4]. При этом должен соблюдаться баланс между соблюдением требований безопасности, призванных оградить проникновение в ИС злоумышленников, и удобством, а

1 Сабанов Алексей Геннадьевич, эксперт ISO/JC1/SC27/WG5, член ТК-362, ТК-122, кандидат технических наук, доцент МГТУ им. Н.Э. Баумана, заместитель генерального директора ЗАО «Аладдин Р.Д.» г. Москва, Россия. E-mail: asabanov@mail.ru

также простотой доступа для легальных пользователей. В связи с развитием процесса цифровизации борьба за простоту получения доступа привела к тенденции ослабления требований безопасности и, в частности, снижения уровня доверия к результатам ИА. Недостаток четких технических требований и рекомендаций к организации процессов аутентификации приводит к тому, что выбор методов и средств аутентификации отдан на откуп владельцам (операторам) ИС [5]. Для облегчения правильного выбора на основе международных стандартов во многих развитых странах выработаны государственные рекомендации по цифровой идентификации граждан и применению различных методов аутентификации, разделенных по уровням доверия[2] [3]. К сожалению, в нашей стране таких рекомендаций пока не разработано. Анализ указанных рекомендаций и стандартов ISO[4] [5] применительно к практике использования отечественных средств криптографической защиты информации и аутентификации приведен в [6]. Как показано в этой работе, так называемый технологический подход, разработанный американским институтом NIST, применим в условиях развитой нормативной базы и наличия утвержденных методик анализа рисков. Для российских компаний доверие к аутентификации также должно быть подкреплено анализом рисков [7], однако утвержденных и применяемых на практике методов анализа рисков пока явно недостаточно. В условиях достаточно широкого выбора и интенсивного предложения от разработчиков различных технологий ИА владельцев (операторов) ИС интересует вопрос о том, насколько можно доверять результатам ИА при использовании тех или иных средств и методов аутентификации. Акцент на результаты ИА обусловлен интенсивным процессом цифровизации, сопровождающимся взрывным характером роста количества ИС и необходимостью повышения доверия к электронному взаимодействию в целом и электронным сделкам в частности, для чего необходима уверенность в подлинности сторон.

Целью данной работы является разработка концепции формирования уровней доверия к результатам аутентификации на основе анализа рисков, проведенных в работах [8,9]. В качестве основы концепции используются результаты работ [2-8], а также исследования процессов ИА на основе многоуровневой модели рисков [10].

2 Paul A. Grassi, James L. Fenton, Michael E. Garcia. NIST Special Publication 800-63 - 3. Digital Identity Guidelines. Revision 3. June 2017. [Электронный ресурс]: Режим доступа: https://pages.nist.gov/800-63-3/sp800-63-3.html, свободный

3 User Authentication Guidance for Information Technology Systems. ITSP.30.031. v.3. April 2018. Government of Canada.[Электронный ресурс]: Режим доступа: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v3-eng_0.pdf, свободный.

4 ISO/IEC 29003: 2017 Information technology – Security techniques – Identity Proofing [Электронный ресурс] – Режим доступа: https://www.iso.org/ru/standard/62290.html, свободный.

5 ISO/IEC 29115: 2013 Information technology – Security techniques – Entity authentication assurance framework [Электронный ресурс]: Режим доступа: https://www.iso.org/standard/45138.html, свободный.

Краткий анализ международных и национальных стандартов

Одной из тенденций развития стандартов ISO в части ИА в течение последних двух-трех лет является ориентир на документы, разработанные институтом NIST США[2]. Так, последняя версия основного стандарта ISO по аутентификации[5] полностью базируется на требованиях NIST SP 800-63-3, состоящего из четырех частей[2].

Изложим принцип использования предложенных в США и Канаде уровней доверия.

На основе собственных оценок риска ошибок подтверждения идентификационных данных, аутентификации и федеративной интеграции по отдельности (чтобы определять необходимый уровень доверия для каждой типовой транзакции) организация выбирает следующие отдельные уровни доверия:

IAL (Identification Assurance Level – уровень доверия к идентификации) служит для повышения надежности процесса подтверждения идентификационных данных и выбирается для уменьшения потенциальных ошибок подтверждения идентификационных данных;

AAL (Authentication Assurance Level – уровень доверия к аутентификации) предназначен для повышения надежности процесса аутентификации и связи между АИ и идентификатором конкретного субъекта доступа, а выбирается для уменьшения потенциальных ошибок аутентификации;

FAL (Federation Assurance Level – уровень доверия к федеративной интеграции) используется при необходимости повышения безопасности и надежности передачи АИ и информации об идентификационных атрибутах стороне, предоставляющей доступ.

Международные[4] [5] и национальные[2] [3] стандарты рекомендуют организациям и агентствам бюджетной сферы следующий порядок действий:

1. Организация должна выполнить оценку рисков ошибок подтверждения идентификационной информации, предоставленной претендентом на право нового пользователя ИС, а также оценку рисков ошибок аутентификации для типовых онлайн-транзакций.
2. Определяются остаточные и приемлемые риски.
3. В зависимости от соотношения остаточных и приемлемых рисков выбирается уровень доверия к идентификации (IAL) и уровень аутентификации (AAL), процессы, технологии и методы, соответствующие каждому выбранному уровню доверия. При существенном превышении остаточных рисков над приемлемыми уровень доверия может быть повышен, или часть рисков должна быть перенесена на третью сторону (например, на страховую компанию).

Для простоты обычно вводятся всего три уровня доверия: низкий, средний, высокий. Однако в зависимости от назначения ИС и состава обрабатываемой информации каждый из перечисленных уровней может быть разбит на подуровни, как показано в [3].

Доверие к идентификации

В работе [2] подробно рассмотрен вопрос формирования доверия к результатам идентификации (ДРИ).

УДК 004.056.52 DOI: 10.21681/2311-3456-2019-5-19-25

Показано, что ДРИ главным образом определяется организацией процесса и результатами первичной идентификации (ПИ).

Показано, что доверие к результатам ПИ может достигаться комплексом мер:

а) сбор и распознание предоставленной заявителем информации;

б) проверка подлинности предоставленных заявителем свидетельств, содержащих идентификационные атрибуты;

в) проверка достоверности идентификационных атрибутов и их значений;

г) верификация минимально-достаточных для идентификации атрибутов;

д) проверка степени привязки идентификационных атрибутов к заявителю;

е) протоколирование и хранение результатов проверок и верификации.

При этом должны учитываться риски нарушения конфиденциальности и целостности собранных персональных данных и условия защиты этой информации при обработке и передаче.

Составляющие доверия к идентификации

Составляющие доверия к результатам электронной идентификации субъекта (объекта) доступа в работе [2] сформулированы следующим образом:

1. качество первичной идентификации;
2. безопасность обрабатываемой, хранимой и передаваемой в процессе первичной идентификации информации (конфиденциальность, целостность, аутентичность и доступность персональных данных);
3. достоверность связи конкретного субъекта доступа с предоставленной им идентификационной информацией;

где под качеством ПИ понимается результат проверки уникальности предоставленной претендентом ИД, достигнутый уровень верификации этих ИД в государственных электронных реестрах, а также отсутствие сбоев и ошибок в работе СИА. Все указанные три критерия могут быть представлены в виде безразмерных функций, значения которых позволяют оценить реальный уровень ДРИ.

Доверие и риски аутентификации

Как уже упоминалось во введении, целью аутентификации в каждой ИС является определение, является ли стремящийся получить доступ субъект тем зарегистрированным пользователем, за кого себя выдает. При этом ключевым словом является «зарегистрированным», то есть после регистрации система аутентификации оперирует только с теми данными, которые остались в ней после регистрации нового пользователя.

Следовательно, формально доверие к процессу аутентификации и его практической реализации не зависит от качества проведения регистрации, но на конечный результат работы СИА качество регистрации и особенно ПИ оказывает весьма существенное влияние. Заметим, что ответ на вопрос связи личности пользователя с его уникальным идентификатором (например, в простейшем случае - логином) и зарегистрированной АИ (в простейшем случае – паролем) определяется выполнением требований ИС к регистрации нового пользователя. Например, если для регистрации достаточно предъявить копию паспорта, то доверие к этой связи будет практически нулевое, поскольку в копию с помощью современных средств техники легко могут быть внесены изменения в данные, к примеру, может быть заменена фотография. Различные аспекты доверия к результатам аутентификации рассмотрены в работах [16-21]. Основываясь на результатах работ [22-26] можно сделать вывод о том, что составляющими доверия могут быть функциональная надежность работы СИА, достоверность результатов ИА и безопасность АИ и идентификационных данных. При этом основным инструментом анализа является оценка рисков. Как показано в работах [19,20], доверие в ИС обратно пропорционально рискам. Риски аутентификации подробно рассмотрены в работах [7,8], основанных на анализе применимости методов оценки рисков [7] и предложенных в [10] модели и методики оценки рисков [4]. В качестве основного вывода из рассмотренных 12 опасных событий в работе [9] установлено два наиболее критичных для достижения заданного уровня доверия к результатам аутентификации. Первое связано с необходимостью защиты от несанкционированного доступа АИ на протяжении всего жизненного цикла. Второе – с правильным выбором метода аутентификации, определяемого сочетанием факторов аутентификации, способов обмена АИ и применяемого протокола обмена претендент – сервер аутентификации.

Методы аутентификации

Методы аутентификации подробно рассмотрены в работе [27], где определены уровни доверия к наиболее широко применяемым методам (рис.1).

Оценка доверия к результатам аутентификации

На основании выполненных исследований предлагается метод оценки доверия к результатам аутентификации субъекта доступа в пространстве безразмерных параметров, где обобщенная функция доверия Ψ может быть представлена в виде:

$$\frac{\varphi_p}{p}\ \frac{\varphi_{кс}}{R_{кс}}\ \frac{\varphi_{ма}}{R_{ма}}),$$

где φ_p – показатель качества результата регистрации нового субъекта доступа, $\varphi_{кс}$ – показатель защищенности аутентифицирующей информации (конфиденциальности секрета), $\varphi_{\text{ма}}$ – показатель корректности реализации метода аутентификации, R_p – величина суммарного риска при регистрации, $R_{кс}$ – величина суммарного риска при генерации, хранении, использовании и утилизации конфиденциальности секрета, – величина суммарного риска при реализации метода аутентификации. Обобщенная функция доверия пока недостаточно исследована. По определению она может изменяться в пределах $0 \le \Psi \le 1$. Поясним физический смысл этой функции. Чем ближе получаемая в результа-

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Вид аутентификации	Уровень доверия к результату аутентификации
1	запоминаемый секрет (примеры: пароль, PIN-код)	пароль	защита пароля от известных атак	односторонний	знание	простая	низкий
2	сгенерированный заранее одноразовый пароль, записанный на носителе (пример: скрэтч-карта)	одноразовый пароль	доверенный ДСЧ, защита канала распределения OTP, защита от MitM-атак	односторонний	владение		
3	"второй канал" (пример: телефон+SMS)	одноразовый пароль	защита операций аутентификации в обоих каналах	односторонний	владение		средний
4	устройство одноразовых паролей, динамически генерирующая OTP	одноразовый пароль	защита устройства	односторонний	владение		
5	многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия	усиленная	высокий
6	криптографическй ключ в СВТ или на незащенном паролем носителе	криптографические ключи	защита ключей	односторонний или взаимный	владение		
7	устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание		
8	СВТ с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	строгая	очень высокий
9	СВТ с криптографическим ПО и отдельное устройство с помещённым и хранящемся в нём криптографическим ключом + доступ к ключу по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия		
10	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия		самый высокий

Рис.1. Методы аутентификации и уровни доверия

те оценок поверхность функции Ψ к границам единичного куба с направляющими, характеризующими показатели качества регистрации, защищенности аутентифицирующей информации и реализации соответствующего метода аутентификации, отнесенными к соответствующим рискам, тем больше может быть уверенность в достоверности, надежности и безопасности полученных результатов аутентификации субъекта доступа.

Критерии доверия к результатам идентификации и аутентификации

На основе анализа результатов перечисленных выше работ автора можно заключить, что доверие к результатам идентификации и аутентификации (ДРА) складывается из:

- доверия к надежности результатов регистрации нового пользователя (характеризующего качество ПИ) - насколько присвоенный уникальный в данной информационной системе идентификатор и соотнесенные с ним идентификационные данные соответствуют субъекту, т.е. насколько достоверно определено, что заявитель является тем субъектом, за кого себя выдает;
- доверия к обеспечению конфиденциальности секрета (аутентифицирующей информации) на протяжении всего его жизненного цикла. Примеры: пароль в случае простой аутентификации или закрытый ключ доступа в случае строгой аутентификации – условия его генерации, хранения, использования, утилизации;
- доверия к корректности реализации методов аутентификации, включающих в себя организацию обмена аутентификационной информации между заявителем и сервером аутентификации (односторонний или взаимный обмен), используемые при этом факторы аутентификации и протоколы обмена. Факторы аутентификации подвержены атакам (пароль – подбор или перехват, ключевой носитель с секретом можно украсть, биометрию можно эмулировать). Протоколов аутентификации разработано более десяти, планируемый к использованию протокол должен соответствовать заданному уровню доверия к методу аутентификации.

Формирование уровней доверия к идентификации и аутентификации

Как показано в работе [27], на итоговый уровень доверия существенное влияние оказывает соотношение уровней доверия к результату идентификации и аутентификации.

Указанные уровни доверия должны согласовываться между собой. Поясним это на простом примере. Если для определенных транзакций применяется строгая взаимная многофакторная аутентификация и используемая аутентификационная информация прекрасно защищена, но регистрация нового пользователя проводится только по копии паспорта, итоговый уровень доверия к результатам ИА практически равен нулю.

УДК 004.056.52 DOI: 10.21681/2311-3456-2019-5-19-25

	Низкий уровень доверия к результатам идентификации	Средний уровень доверия к результатам идентификации	Высокий уровень доверия к результатам идентификации
Низкий уровень доверия к результатам аутентификации	Низкий уровень доверия	Низкий уровень доверия	Низкий уровень доверия
Средний уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Средний уровень доверия
Высокий уровень доверия к результатам аутентификации	Низкий уровень доверия	Средний уровень доверия	Высокий уровень доверия

Заключение

Аутентификация пользователей крайне важна для противодействия проникновению злоумышленников в информационные системы, а меры защиты информации, используемые для защиты ИС, представляют собой важнейшие элементы при разработке ИТ - инфраструктуры. Определение методов управления доступом, необходимых для защиты информации и услуг, в частности, аутентификации, является обязанностями организации в рамках структуры менеджмент риска. В данной работе собраны основные результаты долголетних исследований автора, предназначенные оказать помощь в выборе методов идентификации и аутентификации при построении систем ИА. В развитие работы будут рассмотрены проблемы применения в целях ИА биометрических методов идентификации на стационарных рабочих местах и с применением мобильных устройств.

Литература

1. Грушо А. А., Забежайло М. И., Смирнов Д. В., Тимонина Е. Е. О комплексной аутентификации // Системы и средства информ., 27:3 (2017), С. 4–11.
2. Сабанов А.Г. Критерии доверия к результатам идентификации субъектов доступа // Электросвязь. 2019. №3. С.38-44.
3. Сабанов А.Г. Способ определения строгости аутентификации// Электросвязь. 2016. №8. С.56-61.
4. Сабанов А.Г. Формирование уровней доверия к идентификации и аутентификации субъектов при удаленном электронном взаимодействии // Электросвязь. 2015.№10, С.46-51.
5. Сабанов А.Г. Обзор иностранной нормативной базы по идентификации и аутентификации // Инсайд. Защита информации. 2013. №4(52), с.82-88.
6. Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 1 // Инсайд. Защита информации. Часть 1. 2016. №2(68). С.84-87. / Часть 2. 2016.№3, С.70-73.
7. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь 2014. №5. С.44-47.
8. Сабанов А.Г. О применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь 2014. №6. С.39-42.
9. Минаев В.А., Королев И.Д., Сабанов А.Г. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия // Вестник УрФО. Безопасность в информационной сфере. 2018. №3(30). С.43-49.
10. Сабанов А.Г. Метод многоуровневого анализа рисков аутентификации при удаленном электронном взаимодействии // Вопросы защиты информации. 2014. №2. С.29-36.
11. Сабанов А.Г. О неизвлекаемости закрытых ключей // Инсайд. Защита информации. 2015. №2. С.30-33.
12. Сабанов А.Г. Доверенные системы как средство противодействия кибер-угрозам // Инсайд. Защита информации. 2015. №3. С.17-21.
13. Paul A. Grassi, James L. Fenton, Michael E. Garcia. NIST Special Publication 800-63 - 3. Digital Identity Guidelines. Revision 3. June 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html
14. Конявский В.А. Проблемы доверия к результатам идентификации и аутентификации в финансовых организациях // Information Security / Защита информации. 2017. №5. С.24-26.
15. Paul A. Grassi, James L. Fenton. NIST Special Publication 800-63A Digital Identity Guidelines. Enrollment and Identity Proofing Requirements. June 2017. https://pages.nist.gov/800-63-3/sp800-63a.html
16. Маллаев Ш.Р. Использование методов аутентификации в развитии электронной торговли // Вопросы структуризации экономики. 2014. № 2. С. 80-85.

17. Никитин В.В., Гунченко Ю.И., Басов О.О. Оценка условных вероятностей байесовской сети доверия при априорной информации о взаимодействии между ее узлами в системе многомодальной аутентификации пользователя // Научный результат. Информационные технологии. 2017. Т. 2. № 3. С. 3-10.
18. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation // System Sciences. 2002. P. 2431-2439.
19. Шиверов П.К., Бондаренко В.В. Понятие доверия в контексте информационной безопасности // Информационные технологии и нанотехнологии-2016. – 2016. – с. 414–418.
20. Шиверов П.К., Новосад Т.Г., Осипов М.Н. Доверие в контексте анализа стойкости протоколов аутентификации // Ползуновский вестник. 2014. № 2. С. 248-250.
21. Шведова Л.Е. Средства защиты доступа к информационным системам // Математические методы и информационно-технические средства: материалы XI Всероссийской научно-практической конференции (г. Краснодар, 19 июня 2015 г.). С. 318-321.
22. Губка О.А. Как организовать аутентификацию в сети взаимодействующих предприятий. Инсайд. Защита информации. 2018. №2(80). С.75-77.
23. Шубинский И.Б. Надежные отказоустойчивые системы. Методы синтеза / Ульяновск: областная типография «Печатный двор», 2016. – 544с.
24. Сабанов А.Г., Смолина С.Г. Сравнительный анализ биометрических методов идентификации личности. Труды ИСА РАН. Том 66 3/2016. С.12-21.
25. Ермаков А.С., Аманжолова С.Т. Модели аутентификации и идентификации распределенной вычислительной системы на примере системы дистанционного образования // Известия НТО «КАХАК». – 2009. - №1/32. С.11-17.
26. Бобов М.Н. принципы построения систем разграничения доступа в интегрированных телекоммуникационных системах // Российско-Белорусский научно-технический журнал «Управление защитой информации». 2001. Том 5. №3. С.267-273.
27. Сабанов А.Г. Уровни доверия к аутентификаторам // Вопросы защиты информации. 2019. №2. С.10-17.

LEVELS OF CONFIDENCE TO IDENTIFICATION AND AUTHENTICATION RESULTS DURING DIGITAL TRANSFORMATIONS

Sabanov A[6].

Purpose of the article: *the development of the formation concept of credibility levels to citizens' identification and authentication results while moving to digital economy.*

Method: *the synthesis of the concept on the basis of the international standards analysis, identification and authentication processes and also identification and authentication errors risk assessment in tasks of information resources and systems access management.*

The result: the analysis of international and a number of national standards concerning identification and authentication assurance is performed. Identification and authentication and also participants are being analyzed. On the basis of the performed analysis and risk assessment criteria of trust to results of identification and authentication are formulated. It is shown that the trust to identification of the access subject is defined by the citizen's primary identification performance quality, that is reliability of definition of whether the subject is that for whom gives itself. Trust assessment methods to results of primary identification are developed.

It is established that the trust to authentication results is defined by the reached trust to primary identification of the access subject during registration, trust to ensuring of a secret confidentiality (authenticating information) throughout all its life cycle and also trust to implementation correctness of the authentication methods including the organization of authentication information exchange between the applicant and the authentication server (one-sided or mutual exchange), the authentication factors and exchange protocols used at the same time. The trust valuation method to authentication results of the registered access subject in space of dimensionless parameters developed according to the offered trust criteria is given. On the basis of the provided analysis the concept of the trust levels forming to identification and authentication results, different from the known foreign analogs is developed according to specifics of the certified means of cryptographic information protection and authentication means application.

6 Alexey Sabanov, Ph.D. (tech.), Associate Professor of Bauman Moscow State Technical University, Deputy General Director, «Aladdin R.D.» company, Moscow, Russia. E-mail: asabanov@mail.ru

Keywords: primary identification, risks evaluation, authenticating information, method of authentication, level of assurance, assurance criteria, access entity.

References

1. Grusho Alexander A., Zabezhailo Michael I., Smirnov Dmitry V., Timonina Elena E. About Complex Authentication // Systems and Means of Informatics, 27:3 (2017), С. 4–11.
2. Sabanov A.G. Assurance Criteria to Access Entities Identification Results // Telecommunication. 2019. №3. pp.38-44.
3. Sabanov A.G. Assurance Criteria to Access Entities Identification Results // Method for determining the severity of authentication // Telecommunication. 2016. №8. С.56-61.
4. Sabanov A.G. Formation of Assurance Levels for Entities Identification and Authentication in Remote Electronic Interaction // Telecommunication. 2015.№10, pp.46-51.
5. Sabanov A.G. Review of the Foreign Regulatory Framework for Identification and Authentication // Inside. Information Security. 2013. №4(52), pp.82-88.
6. Sabanov A.G. General Analysis of International Standards for Identification and Authentication when Accessing Information // Inside. Information Security. Part 1. 2016. N2(68). pp.84-87. / Part 2. 2016. N3, pp.70-73.
7. Sabanov A.G. Analysis of the Applicability of Risk Assessment Methods to Authentication Processes in Remote Electronic Communication // Telecommunication. 2014. N5. pp.44-47.
8. Sabanov A.G. On the Applicability of Risk Management Methods to the Processes of Authentication for Remote Electronic Interaction // Telecommunication 2014. N6. pp.39-42.
9. Minaev V.A., Korolev I.D., Sabanov A.G. Assessment of Identification and Authentication Risks for Subjects of Electronic Interaction // Bulletin of the Ural Federal okrug. Information Security. 2018. N3(30). pp.43-49.
10. Sabanov A.G. Method Multilevel Authentication Risks Analysis for Remote Electronic Interaction // Information Security Issues. 2014. N2. pp.29-36.
11. Sabanov A.G. On the Non-recoverability of Private Keys // Inside. Information Security. 2015. N2. pp.30-33.
12. Sabanov A.G. Trusted Systems as a Means of Countering Cyber Threats // Inside. Information Security. 2015. N3. С.17-21.
13. Paul A. Grassi, James L. Fenton, Michael E. Garcia. NIST Special Publication 800-63 - 3. Digital Identity Guidelines. Revision 3. June 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html
14. Konyavsky V.A. Problems of Trust in the Results of Identification and Authentication in Financial Institutions // Information Security. 2017. N5. pp.24-26.
15. Paul A. Grassi, James L. Fenton. NIST Special Publication 800-63A Digital Identity Guidelines. Enrollment and Identity Proofing Requirements. June 2017. https://pages.nist.gov/800-63-3/sp800-63a.html
16. Mallaev S.R. The Use of Authentication Methods in the Development of e-Commerce // Issues of economic structuring. 2014. N2. pp. 80-85.
17. Nikitin V.V., Gunchenko Y. I., Basov O.O. Evaluation of Conditional Probabilities of Bayesian Trust Network with a Priori Information about Interaction between its Nodes in the System of Multimodal User Authentication // Scientific result. Information Technology. 2017. T. 2. N 3. pp. 3-10.
18. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation // System Sciences. 2002. P. 2431-2439.
19. Shiverov P.K., Bondarenko V.V. The Concept of Trust in the Context of information Security // Information Technology and Nanotechnology -2016. pp. 414–418.
20. Shiverov P.K., Novosad T.G., Osipov M.N. Trust in the Context of the Analysis of the Resistance of Authentication Protocols // Polzunovskii Vestnik. 2014. N2. pp. 248-250.
21. Shvedova L.E. Protection of Access to Information Systems // Mathematical Methods and Information Technology Tools: Proceedings of the XI all-Russian Scientific-practical Conference (Krasnodar, the 19 of June 2015). pp. 318-321.
22. Gubka O.A. How to Organize Authentication in the Network of Interacting Enterprises. Inside. Information Security. 2018. N2(80). pp.75-77.
23. Shubinsky I.B. Reliable Fault-tolerant Systems. Synthesis method / Ulyanovsk: regional printing house « Printing house», 2016. – 544p.
24. Sabanov A.G., Smolina S.G Comparative analysis of personal identification biometry methods. Proceedings of Institute of System Analysis of Russian Academy of Sciences. Thom 66 3/2016. pp.12-21.
25. Ermakov A.S., Amanzholova C.T. Models of Authentication and Identification of Distributed Computing System on the Example of Distance Education System // News NTO «KAHAK». – 2009. - N1/32. pp.11-17.
26. Bobov M.N. Principles of Construction of Access Control Systems in Integrated Telecommunication Systems // Russian-Belarusian Scientific and Technical Journal «Information Security Management». 2001. Thom 5. N3. pp.267-273.
27. Sabanov A.G. Authenticators Levels of Assurance // Information Security Issues. 2019. N2. pp.10-17.