Отзыв

официального оппонента на диссертационную работу
Сабанова Алексея Геннадьевича
«Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа»,
представленной к защите на соискание ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Актуальность диссертационного исследования Сабанова А.Г. продиктована интенсивной цифровизацией российского общества и экономики. В условиях роста количества информационных систем и киберпреступлений, связанных с таким ростом, диктует необходимость развития научных знаний по проблеме доверия к результатам идентификации и аутентификации субъектов доступа. В отличие от множества публикаций по теме диссертации автор проявил системный подход к выбранной научной проблеме и разработал методологию формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа.

В работе показано, что системы управления доступом и входящие в их состав функциональные блоки идентификации и аутентификации субъектов доступа, стоящие на первом рубеже обороны каждой информационной системы, нуждаются в определении и формировании способов повышения доверия к результатам их работы. Основным инструментом анализа совершенно правильно выбраны методы анализа рисков. Такая научная проблема анализируется в рассматриваемой диссертационной работе.

Целью диссертационной работы автор определяет разработку методологии формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа.

Степень обоснованности научных положений, выводов и рекомендаций рассматриваемой работы опирается на системный подход к

решению поставленных задач, вытекающих из сформулированной цели исследования. В работе критически анализируются известные теоретические положения и научные разработки, а также нормативно-правовые документы. Список литературы содержит 258 наименований. Автор достаточно корректно использует известные научные методы обоснования полученных результатов, выводов и рекомендаций, опирающихся на существующую теоретико-методологическую и нормативно-правовую базы.

Оценка новизны. Научная новизна работы проведенного диссертационного исследования заключается в следующем:

- разработана методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа при электронном взаимодействии на основе моделирования основных процессов и систем идентификации и аутентификации;

- создан новый метод оценки рисков первичной идентификации субъектов доступа, отличающийся от известных применением динамического метода построения матриц рисков первичной идентификации, который позволяет определять величины допустимых рисков и средних значений рисков вероятных опасных событий;

- предложен способ многоуровневой оценки рисков на основе разбиения процесса аутентификации на ряд последовательных связанных процедур;

- проведена оригинальная классификация методов, систем идентификации и аутентификации, а также средств и механизмов аутентификации;

- разработаны вероятностные модели и методики оценки надежности процессов идентификации и аутентификации.

Оценка достоверности. Достоверность результатов работы обеспечивается добротно выполненным анализом современного состояния исследований в предметной области, достаточным обоснованием предложенных методов, моделей и алгоритмов, не противоречащих

известным положениям других авторов. Следует отметить достаточно длинный список из 50 научных публикаций, выполненных автором самостоятельно, и докладов на международных и российских научных и научно-практических конференциях, а также большое количество актов о внедрении. По теме диссертации всего автором опубликовано 67 научных работ в изданиях, рекомендованных ВАК России, в соавторстве опубликовано 3 монографии и 3 учебных пособия.

Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и двух приложений.

Во введении обоснована актуальность темы исследования, сформулированы цель и задачи, перечислены используемые научные методы исследования, указаны объект и предмет исследования, сформулирована научная новизна, выделены пять положений, которые выносятся на защиту, отмечаются практическая и теоретическая ценность полученных результатов.

Первая глава посвящена анализу современного состояния научных работ, международных стандартов, зарубежной и отечественной нормативно-правовой базы по проблемам идентификации и аутентификации. Выявлена необходимость развития новых подходов к решению задач оценивания рисков идентификации и аутентификации, включающих в себя разработку математических моделей, методик и алгоритмов проведения соответствующих оценок. Установлена необходимость введения уровней доверия к результатам идентификации и аутентификации, использование которых может позволить существенно повысить эффективность управления доступом пользователей, в том числе в удаленном режиме, а также сократить сроки проектирования и ввода в эксплуатацию систем идентификации и аутентификации. Обоснована необходимость введения уровней доверия не к процессам, а к результатам идентификации и аутентификации, применение которых позволяет существенно повысить эффективность управления доступом пользователей Сделан вывод, что в качестве показателей доверия могут выступать достоверность идентификационной информации,

функциональная надежность работы системы, безопасность идентификационной и аутентификационной информации, а в качестве основного инструмента для проведения такого исследования должны лежать методы анализа и управления рисками.

Вторая глава содержит методологию формирования уровней доверия к результатам идентификации и аутентификации, а также подробно рассмотрена проблема достоверности и надежности результатов идентификации субъектов доступа в современных и перспективных информационных системах (ИС). Идентификация в условиях роста количества субъектов и объектов в ИС становится сложной задачей и выдвигает новые требования к числу значащих символов идентификаторов и/или их количеству. Установлена зависимость необходимого количества применяемых идентификаторов с известными оценками безошибочности идентификации от числа зарегистрированных в ИС субъектов и объектов доступа. Выполнен структурно-функциональный анализ процессов идентификации. Предложены модели и разработана методика оценки функциональной надежности идентификации. Приведены методы оценки надежности первичной идентификации, а также оценки ошибок идентификационной информации и ошибок при верификации, а также при передаче идентификационной информации.

Сформулированы цели, задачи и требования к первичной и вторичной идентификации. Установлено, что доверие к результатам идентификации определяется главным образом результатами первичной идентификации. Доверие к результатам первичной идентификации в свою очередь, зависит от достигнутого доверия к результатам проверки уникальности предъявленных заявителем идентификационных атрибутов, доверия к результатам верификации этих идентификационных атрибутов и доверия к привязке идентификационной информации к конкретной личности заявителя. Предложены три уровня доверия к результатам идентификации субъектов доступа. Примечательно, что указанные положения вошли в ГОСТ Р 58833-

2020 «Идентификация и аутентификация. Общие положения» и в проект ГОСТ Р ХХХ-2020 «Идентификация и аутентификация. Уровни доверия к результатам идентификации», куда также введены основные понятия и основные положения организации процессов идентификации с целью достижения определенных уровней доверия к полученным результатам.

Впервые проведена оценка рисков первичной идентификации. Рассмотрены типовые угрозы и возможные атаки, идентифицированы основные риски первичной идентификации, которые согласно ГОСТ Р 31010 рассмотрены в виде набора вероятных опасных событий (ВОС). Для этого набора ВОС построены матрицы рисков, анализ которых позволил определить уровни допустимых рисков для трех наиболее распространенных типов информационных систем (ИС): закрытых (корпоративных), открытых ИС с личной явкой нового пользователя к регистратору и открытых ИС без личной явки субъекта к регистратору. Установлено, что уровень рисков первичной идентификации для открытых систем на порядок выше, чем для корпоративных, при этом наибольший риск представляет регистрация нового пользователя в удаленном режиме без личного присутствия. Представлены оценки средних значений рисков по отношению к допустимому уровню рисков для всех рассмотренных комбинаций. На основе проведенных исследований сформулированы критерии доверия и приведен способ оценки доверия к результатам идентификации в соответствии с предложенными критериями для ИС различного назначения.

Проведена оценка надежности первичной идентификации субъектов доступа для больших информационных систем. Показана необходимость учета соотношения количества зарегистрированных пользователей и объектов в системе к числу используемых при доступе пользователей идентификаторов.

Третья глава диссертационной работы посвящена проблеме оценки доверия к результатам аутентификации субъектов доступа. Выполнен анализ архитектуры и типовых схем систем идентификации и аутентификации

(СИА) для закрытых корпоративных ИС и ИС общего пользования с целью выявления типовых особенностей их функционирования для последующего исследования и моделирования. Разработана оригинальная классификация СИА по критериям выполнения целей обеспечения доступности, целостности и конфиденциальности, показывающая многообразие задач и вытекающих из них требований к безопасности и надёжности СИА. Показано, что проектирование, построение, поддержка и развитие СИА, а также выбор и внедрение средств идентификации и аутентификации должны базироваться на циклическом анализе рисков. Установлено, что в целях обеспечения доступности, достоверности результатов и отказоустойчивости на этапах проектирования и совершенствования СИА должны исследоваться с помощью методов теории массового обслуживания, теории функциональной надежности и безопасности.

Рассмотрены основные информационные потоки и участники процессов идентификации и аутентификации пользователей при удаленном электронном взаимодействии, в том числе при переходе к облачным вычислениям, с целью определения методов анализа безопасности и надёжности как самих процессов, так и формируемой, передаваемой, хранимой и обрабатываемой идентификационной и аутентификационной информации. В виде основного инструмента анализа определён анализ рисков с помощью нисходящих и восходящих методов. Сделан вывод о необходимости декомпозиции процедур и процессов аутентификации для уточнения количественных значений рисков. Определены последовательность процедур, составляющих процесс аутентификации, участники электронного взаимодействия и основные информационные потоки в процессах аутентификации с целью их последующего моделирования для анализа рисков и оценки надёжности.

Разработана классификация технологий и средств идентификации и аутентификации по признакам выполнения основных целей, функций и обеспечения безопасности, а также для определения границ областей

применения наиболее развитых технологий аутентификации по критериям цели, задач и степени защищённости электронного взаимодействия.

На основе анализа рисков сформулированы критерии доверия к результатам аутентификации, что позволило разработать методологию построения уровней доверия к результатам аутентификации в зависимости от достигнутого уровня доверия к результатам первичной идентификации, применяемых методов аутентификации, способа генерации, хранения и предъявления аутентификационной информации и уровней требований информационной безопасности к работе самой системы идентификации и аутентификации, а также защите идентификационных атрибутов, являющихся персональными данными. Предложен способ оценки доверия к результатам аутентификации зарегистрированного субъекта доступа в пространстве безразмерных параметров, разработанный в соответствии с предложенными критериями доверия. На основе выполненного анализа разработана методология формирования уровней доверия к результатам идентификации и аутентификации, отличающаяся от известных зарубежных аналогов учетом специфики применения сертифицированных средств криптографической защиты информации и средств аутентификации.

В четвертой главе представлены примеры применения основных положений данной работы к различным теоретическим и практическим задачам. Приведенные примеры внедрений разработанных и модернизированных в данной работе методов и методик анализа процессов идентификации и аутентификации показывают как научный, так и прикладной характер рассматриваемого исследования. Разработанная многоуровневая система оценки рисков идентификации и аутентификации предоставляет возможности дойти до необходимого уровня детализации оценок достигнутого уровня доверия, что позволило, например, создать с участием автора ряд сертифицированных средств защиты информации.

Разработаны типовые требования к аутентификации определенных групп пользователей для достижения определенных уровней доверия. Для

государственных информационных систем рекомендовано введение, как минимум, трех уровней доверия.

Рассмотрена задача обеспечения юридической силы и юридической значимости электронных документов. Показано, что аналогом реквизитов бумажных документов являются сервисы безопасности, применяемые для создания, оформления и подписи электронного документа. Установлен минимальный набор сервисов безопасности: аутентификация, электронная подпись, метка доверенного времени, валидация сертификата ключа проверки подписи, проверка полномочий лица, подписавшего документ, гарантированная доставка документов и сообщений.

Из заключения, приведенного автором работы, в рамках решения поставленной научно-технической проблемы можно отметить следующие результаты:

1. Сформулированы показатели доверия к результатам идентификации и аутентификации. Установлено, что доверие к результатам идентификации в задачах управления доступом пользователей определяется главным образом уровнем доверия, достигнутым при первичной идентификации заявителя во время его регистрации в конкретной ИС. Доверие к результатам первичной идентификации зависит от достигнутого доверия к результатам проверки уникальности предъявленных заявителем идентификационных атрибутов, доверия к результатам верификации этих идентификационных атрибутов и доверия к привязке идентификационной информации к конкретной личности заявителя. Доверие к результатам аутентификации зависит от качества первичной идентификации при регистрации, способа генерации, хранения и использования аутентификационной информации (секрета), а также методов аутентификации (протоколов, применяемых для аутентификации, количества используемых факторов и способов обмена аутентификационной информацией). Таким образом, в работе содержатся основные положения, методы и модели для совершенствования способов защиты информации применительно к задаче идентификации и аутентификации участников

электронного взаимодействия, позволяющие проводить оценку рисков, достоверности, надежности, безопасности и на их основе формировать уровни доверия к результатам идентификации и аутентификации.

2. Формализованы процедуры первичной и вторичной идентификации, разработаны методики и модели анализа достоверности, безопасности и надежности идентификации при удаленном взаимодействии на основе анализа рисков, позволяющие определить требования к первичной идентификации в ИС с большим числом субъектов доступа.

3. Разработан метод оценки рисков первичной идентификации для корпоративных ИС и систем открытого типа с личной явкой субъекта к регистратору и в удаленном режиме, без личной явки. Приведены оценки рисков для указанных типов ИС. Построены матрицы рисков первичной идентификации, что позволяет существенно повысить обоснование результатов анализа рисков на основе определенных из матриц рисков допустимых уровней рисков для типовых вероятных опасных событий.

4. Для оценки рисков аутентификации разработаны и модернизированы модели и методики, позволяющие проводить анализ рисков с необходимой глубиной детализации для ИС различного назначения. Разработаны многоуровневые модели и методы анализа рисков нарушения безопасности информации, включающие в себя рассмотрение угроз, уязвимостей, нежелательных событий и возможных последствий. Рекомендованы два метода управления рисками аутентификации – экономический и вероятных опасных событий.

5. Разработаны вероятностные модели и методики оценки функциональной надежности процессов идентификации и аутентификации, а также методика оценки достоверности результатов при удаленном электронном взаимодействии, что позволяет формировать уровни надежности результатов идентификации и аутентификации.

6. На основе предложенной методологии и разработанных методов, моделей и методик решён ряд практических задач, позволяющих существенно

повысить уровень защищённости информационных ресурсов Российской Федерации. На базе проведенного анализа международных стандартов и нормативной базы, а также принятого стандарта ГОСТ Р 58833 «Идентификация и аутентификация. Общие положения», созданного с использованием положений диссертационной работы, под руководством и с непосредственным участием автора разрабатывается серия национальных стандартов по идентификации и аутентификации.

7. Применение полученных научных результатов на стадиях проектирования и эксплуатации систем идентификации и аутентификации согласно актам о внедрении позволяет существенно сократить сроки проектирования и/или модернизации существующих ИС, снизить затраты на администрирование системы управления доступом и сократить количество инцидентов нарушений безопасности, связанных с идентификацией и аутентификацией.

Таким образом, в диссертационной работе А.Г. Сабанова решена крупная научная проблема, имеющая существенное теоретическое и прикладное значение.

По содержанию работы имеются и некоторые замечания.

1. По работе в целом. Несмотря на системность изложения, несколько нарушен баланс содержания и объема глав работы. Следует отметить, что значительная часть первой главы посвящена рассмотрению международных стандартов, читается легко, как говорится, «на одном дыхании», но носит главным образом описательный, а не исследовательский характер; ее можно было бы немного сократить, это нисколько не умалило бы достижений автора. Вторая и третья главы самые важные по содержанию и новизне, в то же время занимают и самый большой совместный объем в 180 страниц, это половина всего напечатанного текста. Четвертая глава сильно урезана – такое ощущение, что автор сократил ее до минимума, пытаясь уложиться в заданный общий объем, хотя в этой главе рассматриваются весьма

важные и интересные примеры практического применения рассматриваемой методологии.

2. По тексту работы много внимания уделено проблемам функциональной надежности, достаточно полно рассмотрена проблема достоверности идентификации. В то же время проблемы защиты персональных данных при идентификации и аутентификации практически не исследованы.
3. Нуждается в дальнейшей проработке вопрос о количественных показателях уровней доверия. В качестве пожелания хотелось бы увидеть показатели уровней доверия к результатам идентификации и аутентификации субъектов доступа в цифровых значениях. Тогда можно было бы сформулировать критерии отнесения рассматриваемых решений к тому или иному уровню доверия и соотнести их, например, с уровнями защиты от НСД информационных ресурсов, к которым разрешен доступ субъекту.

Отмеченные недостатки несколько снижают качество проведенного исследования, но не влияют на главные теоретические и практические результаты работы.

Автореферат отражает основные положения диссертационной работы, материалы диссертации достаточно полно освещены в публикациях автора.

В целом диссертационная работа Сабанова А.Г. «Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа» представляет собой целостную научную работу, в которой автором разработаны теоретические основы, методы и алгоритмы, имеющие важное хозяйственное значение.

Считаю, что диссертационная работа Сабанова А.Г. «Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа» соответствует пункту 9 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. (ред. от 02.08.2016). Автор работы

Сабанов Алексей Геннадьевич заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Официальный оппонент,
доктор технических наук (05.13.19), доцент, заведующий кафедрой «Комплексная защита информации» Ложников Павел Сергеевич

ФГБОУ ВО «Омский государственный технический университет»
644050, г. Омск, пр-т. Мира, д. 11
Телефон: 8 (3812) 62-87-07
E-mail: lozhnikov@mail.ru