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. Диссертационная работа Сабанова А.Г. посвящена важной, но пока малоизученной проблеме доверия к результатам идентификации и аутентификации субъектов доступа. В эпоху бурного развития процессов цифровизации надежно определять того, кто находится на другой стороне электронного взаимодействия, весьма актуально. Рассматриваемая диссертация является основательным трудом, имеющим большое значение для развития теории защиты информации в части исследования процессов идентификации и аутентификации субъектов доступа.

Работа состоит из введения, 4 глав, заключения, используемых терминов, списка сокращений и списка литературы из 258 наименований, а также двух приложений. Общий объем работы – 345 страниц.

Целью диссертационной работы автор определяет разработку концепции, теоретических основ, методов и алгоритмов формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии.

Научная новизна работы и полученных результатов 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;

- разработан 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 последовательно связанных процедур, что позволило определять вероятностные характеристики разнородных по длительности и повторяемости

процедур идентификации и аутентификации в корпоративных и открытых ИС;

- проведена оригинальная классификация методов, систем идентификации и аутентификации, а также средств и механизмов аутентификации для выявления границ применимости различных технологий идентификации и аутентификации по критериям целей и задач обеспечения доступности, конфиденциальности и целостности идентификационных и аутентификационных данных пользователей ИС, отличающаяся от известных полнотой выбора критериев, что обеспечило возможность многоуровневого анализа рисков процессов и транзакций в системах идентификации и аутентификации, позволяющего оценивать риски с заданным уровнем детализации;

- разработаны вероятностные модели и методики оценки надежности процессов идентификации и аутентификации, отличающиеся от известных тем, что оценивался не отказ оборудования, а отказ в услугах, что в соответствии с многоуровневым принципом исследования позволяет проводить оценку функциональной надежности как систем идентификации и аутентификации целиком, так и выполняемых процессов, а также отдельных процедур, таких как первичная идентификация участников удалённого электронного взаимодействия.

Достоверность результатов и обоснованность научных положений, результатов и основных выводов работы обеспечивается многосторонним анализом современного состояния исследований в предметной области, системным обоснованием предложенных методов, моделей и алгоритмов, не противоречащих известным положениям других авторов, достаточной апробацией основных положений диссертации в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, а также подтверждается положительным эффектом от внедрения, что подтверждается необычно большим количеством актов (19) о внедрении в организации различного подчинения. По теме представленной диссертации автором опубликовано 67 научных работ в изданиях, рекомендованных ВАК России, в соавторстве опубликовано 3 монографии и 3 учебных пособия.

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

В первой главе автор приходит к выводу о необходимости 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. В качестве показателей доверия предложены достоверность идентификационной информации, функциональная надежность работы системы, безопасность идентификационной и аутентификационной информации, а в качестве основного инструмента для проведения исследования должны лежать методы анализа и управления рисками.

Также автор подчеркивает потребность разработки новых подходов, методов и моделей, адаптированных к проведению анализа функциональной надежности работы системы идентификации и аутентификации как информационной подсистемы управления доступом организации.

Во *второй главе* приведена концепция общей методологии формирования уровней доверия и подробно рассмотрена проблема оценки доверия к результатам идентификации субъектов доступа в современных и перспективных информационных системах. Идентификация в условиях роста количества субъектов и объектов в ИС становится сложной задачей и выдвигает новые требования к числу значащих символов идентификаторов 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 надежности идентификации.

Введены понятия первичной и вторичной идентификации. 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 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. Указанные положения вошли в первый национальный стандарт 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.

В диссертации 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. Разработан способ оценки доверия к результатам идентификации в соответствии с предложенными критериями для ИС различного назначения.

Выполнена 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.

Представленные в главе методы, модели и алгоритмы позволяют сделать вывод о создании методологии формирования иерархии доверия к результатам идентификации.

Третья глава работы посвящена проблеме формирования уровней доверия и оценки доверия к результатам аутентификации субъектов доступа. Выполнен анализ архитектуры и типовых схем систем идентификации и аутентификации (СИА) для закрытых корпоративных ИС и информационных систем общего пользования с целью выявления типовых особенностей их функционирования для последующего исследования и моделирования. Разработана **авторская 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

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 способ 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. **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.

Примеры внедрений разработанных и модернизированных в данной работе методов и методик анализа процессов идентификации и аутентификации показывают не только научный, но и прикладной характер данного исследования.

Из заключения, приведенного автором диссертационной работы, в рамках решения поставленной научно-технической проблемы следует 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. Показано, что 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 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 (на 35%-45%) сократить сроки проектирования и/или модернизации существующих ИС, снизить затраты на администрирование системы управления доступом на 25%-40% и сократить количество инцидентов нарушений безопасности, связанных с идентификацией и аутентификацией, на 15-30%.

Представленные автором материалы позволяют сделать вывод, что в диссертационной работе А.Г. Сабанова решена крупная научная проблема, имеющая существенное теоретическое и прикладное значение. Работа написана хорошим литературным языком, практически нет орфографических и стилистических ошибок, читается легко и оставляет хорошее впечатление. Не вызывают сомнение самостоятельность автора (более 50 публикаций, написанных А.Г. Сабановым единолично), актуальность работы, достоверность приведенной информации и результатов работы, подтвержденная

непротиворечивостью известным фактам и научным результатам, а также внушительным количеством докладов на научных конференциях различного уровня.

Однако имеется и ряд замечаний.

1. При анализе существующих методов и средств, предназначенных для оценки доверия к процессам идентификации, аутентификации, уделяется большое внимание международным и отечественным стандартам, меньше рассматриваются формальные логические модели такие, как, например, логика доверия BAN, предложенная авторами Бэрроуз, Абади, Нидхэм для аутентификации криптографических протоколов.
2. Недостаточное внимание уделено аппаратной составляющей идентификации, аутентификации, современным интеллектуальным устройствам, таким, как электронные ключи, токены, смарт карты, которые играют существенную роль при рассмотрении процессов идентификации и аутентификации.
3. Выполненные автором оригинальные классификации систем, методов, технологий и средств аутентификации входят в состав защищаемых положений, в автореферате достаточно поясняющих рисунков, но в заключении автореферата они не представлены.
4. На смену Концепции обеспечения кибербезопасности в настоящее время с учетом приказа ФСТЭК России от 14.03.2014 № 31 осуществляется переход к более современной Концепции киберустойчивости критически важной информационной инфраструктуры Российской Федерации. Новая Концепция подразумевает гарантированное достижение поставленных целей и задач при наличии как известных, так неизвестных угроз безопасности. Какие новые требования к оценке и достижению определенного уровня доверия к результатам идентификации и аутентификации при этом необходимо сформулировать?

Замечание по оформлению: слишком большое количество сокращений затрудняет восприятие материала при чтении диссертации.

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. В данной работе решена научная проблема, имеющая важное социально-экономическое и хозяйственное значение для развития цифровизации нашей страны. Считаю, что диссертационная работа Сабанова А.Г. «Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа» соответствует пункту 9-14 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. (ред. от 02.08.2016), а 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,
профессор,
доктор технических наук,
профессор кафедры «Безопасность информационных технологий»
Южного федерального университета Бабенко Людмила Климентьевна

25.10.2020 г.

ул. Большая Садовая, 105/42
г. Ростов-на-Дону, 344006
тел. +7 (863) 436-15-18
e-mail: lkbabenko@sfedu.ru

Подпись Л.К. Бабенко удостоверяю.
Директор ИКТИБ Южного федерального университета

26.10.2020 Веселов Геннадий Евгеньевич

Дата, МП