ОТЗЫВ

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

Актуальность исследования. Важнейшим аспектом организации и ведения защиты информации в информационных системах (ИС) является разграничение доступа к защищаемой информации, одним из способов которого, наиболее широко применяемым на практике, является идентификация и аутентификация пользователей ИС и процессов обработки информации. Проведенные до настоящего времени научные работы преимущественно были посвящены решению частных задач, касающихся изысканию мер идентификации и аутентификации, и практически не затрагивали вопросы доверия к ним. Это обусловило то, что фактически до сих пор не было научно обоснованных требований к указанным мерам, а пути такого обоснования не прорабатывались из-за отсутствия соответствующей методологии. Кроме того, принцип дифференциации требований, который сегодня широко применяется при защите информации в ИС, при разработке и применении мер и средств защиты применительно к мерам идентификации и аутентификации не используется по причине отсутствия методологии формирования иерархии уровней доверия к результатам идентификации и аутентификации.

Проблема разработки такой методологии связана с тем, что необходимо, с одной стороны, сформировать теоретические основы оценки рисков идентификации и аутентификации субъектов доступа и на этой основе создать комплекс моделей, методов и алгоритмов для проведения соответствующих оценок надежности и достоверности результатов идентификации и аутентификации, научно обосновать уровни доверия к этим результатам, взаимосвязь уровней доверия к идентификации с уровнями доверия к аутентификации. До сих пор исследования по вопросам идентификации

и аутентификации фактически касались лишь частных задач и не затрагивали аспекты формирования иерархии уровней доверия. Диссертационная работа А.Г. Сабанова в этом смысле является пионерской, а ее тема является крайне актуальной и весьма востребованной практикой.

Цель диссертационной работы автора состояла в разработке методологии формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии.

Судя по содержанию работы и указанному предмету исследований, такая методология должна содержать модели, методы и алгоритмы оценки доверия к результатам идентификации и аутентификации субъектов доступа.

Для достижения поставленной цели автор оценил степень разработанности данной темы и показал, что:

во-первых, проведенные другими авторами исследования в данной области касались лишь отдельных аспектов или процессов, в то время как для оценки доверия к результатам идентификации и аутентификации необходим комплексный анализ, включающий в себя анализ рисков нарушения требований безопасности информации, функциональной надежности выполнения основных процессов и соответствия системы идентификации и аутентификации требованиям доступности, конфиденциальности и целостности обрабатываемой идентификационной и аутентификационной информации пользователей ИС;

во-вторых, для развития теоретических положений и разработки концепции повышения доверия к результатам идентификации и аутентификации необходима формализация описания предметной области, однако для многих факторов и условий, характерных и существенных в области защиты информации для систем идентификации и аутентификации, таких как множество угроз безопасности информации и процессов их реализации, процедур принятия решений по применению мер и средств защиты, наличие характеристик нечисловой природы, сегодня не имеется формальных моделей и пути разработки таких моделей не сформированы. Разнородность, разномасштабность и большое количество подлежащих учету факторов

затрудняют построение адекватных математических моделей и переход к количественным методам их учета при решении задач разграничения доступа;

в-третьих, подходы к оценке доверия сегодня только формируются и далеки от стадии практического применения, а методология обоснования уровней доверия на основе определения допустимых и остаточных рисков отсутствует.

Все это обусловливает наличие научной проблемы создания теоретической и методологической базы построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа, для решения которой в диссертации сформулированы и решались следующие задачи исследований:

1 Разработка концепции формирования иерархии уровней доверия к результатам идентификации и аутентификации субъектов электронного взаимодействия;

2 Создание методологии оценивания достоверности, надежности и безопасности идентификации на основе анализа рисков, позволяющей формировать уровни доверия к результатам первичной идентификации субъектов доступа ИС на основе использования разработанных и известных методов и моделей идентификации;

3 Разработка критериев доверия к результатам первичной идентификации для формирования на их основе подходов к оценке доверия к результатам идентификации субъектов доступа;

4 Формирование комплекса моделей и методов оценки рисков при анализе безопасности аутентификационной информации и функциональной надежности процесса аутентификации; разработка методики оценки рисков, учитывающей участников, порядок и состав основных процедур аутентификации;

5 Создание новых и модернизированных моделей и методов оценки надежности аутентификации субъектов доступа к информационным ресурсам, а также разработка с их использованием критериев доверия и алгоритма оценки доверия к результатам работы систем идентификации и аутентификации на основе анализа безопасности идентификационной и аутентификационной информации, достоверности результатов и надежности работы системы

идентификации и аутентификации, позволяющих в совокупности с решением задач 2–4 создать методологию формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа в информационных системах;

6 Апробация теоретической и методологической базы формирования иерархии уровней доверия к результатам идентификации и аутентификации при решении практических задач, в том числе путем разработки первого национального стандарта по идентификации и аутентификации субъектов доступа, проекта второго национального стандарта, формирующего уровни доверия к результатам цифровой идентификации субъектов доступа, применение методов, моделей и способов оценки доверия к результатам идентификации и аутентификации при решении практических задач построения систем идентификации и аутентификации, разработки новых систем защиты информации и др.

При решении указанных задач автор:

доказал необходимость введения уровней доверия к результатам идентификации и аутентификации в интересах существенного повышения эффективности управления доступом пользователей, в том числе в удаленном режиме, и сокращения сроков проектирования и ввода в эксплуатацию систем идентификации и аутентификации;

предложил систему показателей доверия, к которым отнесены достоверность идентификационной информации, функциональная надежность работы системы идентификации и аутентификации, безопасность идентификационной и аутентификационной информации, а для их расчета – методы анализа и управления рисками;

определил потребность в разработке новых подходов, методов и моделей, адаптированных к проведению анализа функциональной надежности работы системы идентификации и аутентификации как информационной подсистемы защищаемой ИС и основных процессов, происходящих на различных этапах идентификации и аутентификации.

Следует отметить, что, на мой взгляд, рассмотренные в диссертации вопросы оценки надежности функционирования подсистемы идентификации и аутентификации в составе ИС не относятся непосредственно к специальности 05.13.19, вместе с тем комплексное рассмотрение автором проблемы построения иерархии уровней доверия с учетом функциональной надежности указанной подсистемы подчеркивает широту решенной в работе проблемы и ее обусловленность иными факторами, не входящими в круг учитываемых обычно в рамках данной специальности:

показал, что идентификация в условиях роста количества субъектов и объектов в ИС становится нетривиальной задачей и обусловливает новые требования к числу значащих символов идентификаторов или их количеству. Установил зависимость необходимого количества применяемых идентификаторов с известными оценками безошибочности идентификации от числа зарегистрированных в ИС субъектов и объектов доступа, выполнил структурно-функциональный анализ процессов идентификации, предложил модели и разработал методику оценки надежности первичной идентификации, а также оценки ошибок идентификационной информации, ошибок при верификации и при передаче идентификационной информации;

впервые ввел понятия первичной и вторичной идентификации, сформулировал цели, задачи и требования к первичной и вторичной идентификации и установил, 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. 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 разработанные автором основные понятия

и основные положения организации процессов идентификации с целью достижения определенных уровней доверия к полученным результатам;

впервые оценил риски первичной идентификации, при этом им рассмотрены типовые угрозы (в том числе угрозы возможных сетевых атак), идентифицированы основные риски первичной идентификации, которые согласно ГОСТ Р 31010 представлены в виде набора вероятных опасных событий (ВОС). Для этого набора ВОС автор построил матрицы рисков, анализ которых позволил определить уровни допустимых рисков для трех наиболее распространенных типов ИС: закрытых (корпоративных), открытых ИС с личной явкой нового пользователя к регистратору и открытых ИС без личной явки субъекта к регистратору. Установил, что уровень рисков первичной идентификации для открытых ИС 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 условий идентификации. На основе проведенных исследований сформулированы критерии доверия и приведен способ оценки доверия к результатам идентификации в соответствии с предложенными критериями для ИС различного назначения;

оценил надежность первичной идентификации субъектов доступа для больших ИС и показал необходимость учета соотношения количества зарегистрированных пользователей и объектов в системе к числу используемых при доступе пользователей идентификаторов, обосновал вывод о создании методологии формирования иерархии доверия к результатам идентификации;

выполнил анализ архитектуры и типовых схем систем идентификации и аутентификации (СИА) для закрытых корпоративных ИС и ИС общего пользования с целью выявления основных особенностей их функционирования для последующего исследования и моделирования, разработал оригинальную классификацию СИА по критериям выполнения целей обеспечения доступности, целостности и конфиденциальности информации, отражающую многообразие задач и вытекающих из них требований к безопасности и надёжности СИА,

показал, что проектирование, построение, поддержка и развитие СИА, а также выбор и внедрение средств идентификации и аутентификации должны базироваться на циклическом анализе рисков;

рассмотрел основные информационные потоки при идентификации и аутентификации пользователей и процессов, 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, определил, что в виде основного инструмента анализа целесообразно использовать анализ рисков с помощью нисходящих и восходящих методов, обосновал вывод о необходимости декомпозиции процедур и процессов аутентификации для уточнения количественных значений рисков, определил последовательность процедур, составляющих процесс аутентификации, участников электронного взаимодействия и основные информационные потоки в процессах аутентификации с целью их последующего моделирования для анализа рисков и оценки надёжности;

разработал классификацию средств идентификации и аутентификации по признакам выполнения основных целей, функций и обеспечения безопасности и, прежде всего, для определения границ областей применения наиболее развитых технологий аутентификации по критериям выполнения цели, задач и достижения требуемой степени защищённости электронного взаимодействия;

впервые сформулировал на основе анализа рисков 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 к защите идентификационных атрибутов, являющихся персональными данными, предложил способ оценки доверия к результатам

аутентификации зарегистрированного субъекта доступа в пространстве безразмерных параметров, разработанный в соответствии с предложенными критериями доверия, и на основе выполненного анализа разработал методологию формирования уровней доверия к результатам идентификации и аутентификации;

показал возможность применения основных положений и результатов данной работы к различным практическим задачам, в том числе при создании с участием автора защищенного средства отчуждения и переноса информации JaCarta SF ГОСТ, при решении задачи обеспечения юридической силы и юридической значимости электронных документов и обосновании минимально необходимого и достаточного для большинства операций с электронными документами набора сервисов безопасности, при формировании требований к подсистеме идентификации и аутентификации государственных ИС, для которых рекомендовано введение, как минимум, трех уровней доверия и установлено, что самым безопасным с наиболее достоверными результатами методом аутентификации является строгая аутентификация, основанная на цифровом сертификате доступа, при этом самым надежным и безопасным устройством аутентификации является смарт-карта класса SSCD (устройство безопасной генерации ключей электронной подписи) с неизвлекаемыми закрытыми ключами и др.

В ходе исследований автором получены важные научные результаты, обладающие **научной новизной**, к основным из которых, на мой взгляд, относятся следующие:

методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при электронном взаимодействии, на основе моделирования основных процессов и систем идентификации и аутентификации, отличающаяся от известных введением количественных процедур анализа рисков идентификации и аутентификации, в том числе для больших ИС, функционирующих с использованием технологий облачных вычислений, с числом пользователей порядка 10^6;

метод оценки рисков первичной идентификации субъектов доступа с помощью матриц рисков, отличающийся от известных применением динамического метода построения матриц рисков первичной идентификации, который позволяет определять значения допустимых рисков и средних значений рисков вероятных опасных событий;

способ оценки рисков, отличающийся, во-первых, введением нескольких уровней идентификации и аутентификации, во-вторых, разбиением процесса идентификации и аутентификации на ряд последовательных процедур, в-третьих, разработанным автором алгоритмом определения вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в корпоративных и открытых ИС;

оригинальная классификация систем идентификации и аутентификации, а также средств и механизмов аутентификации для выявления границ применимости различных технологий идентификации и аутентификации, отличающаяся от известных введенными автором критериями в соответствии с целями и задачами обеспечения доступности, конфиденциальности и целостности идентификационных и аутентификационных данных пользователей ИС, что обеспечивает возможность оценивания рисков с заданным уровнем детализации;

вероятностно-статистические модели и методики оценки надёжности процессов идентификации и аутентификации, отличающиеся от известных тем, что оценивается не отказ оборудования, а отказ в предоставлении услуги, что в соответствии с многоуровневым принципом анализа позволяет проводить оценку функциональной надежности как системы идентификации и аутентификации в целом, так и выполняемых процессов, а также отдельных процедур, таких как первичная идентификация участников удалённого электронного взаимодействия.

Теоретическая значимость работы состоит в развитии теории и методологии построения иерархии уровней доверия к результатам идентификации и аутентификации участников уделённого электронного взаимодействия, в том числе в условиях применения облачных технологий,

в установлении взаимосвязи рисков нарушения требований разграничения доступа к защищаемой информации с устанавливаемыми уровнями доверия к результатам идентификации и аутентификации, а также в разработке вероятностно-статистических моделей оценки надёжности процессов идентификации и аутентификации.

Практическая значимость результатов работы заключается в том, что:

- во-первых, разработаны научно обоснованные алгоритмы формирования иерархии уровней доверия и оценки доверия к результатам идентификации и аутентификации субъектов доступа, позволяющая использовать их в практической деятельности по построению и модернизации систем управления доступом современных ИС, что подтверждается актами о внедрении их в практическую работу. Применение положений данной диссертационной работы позволяет сократить сроки проведения оценок безопасности, функциональной надежности и достоверности результатов идентификации и аутентификации субъектов доступа на этапах проектирования и эксплуатации ИС различного назначения;

- во-вторых, результаты работы реализованы при разработке автором первых национальных стандартов – ГОСТ Р 58833 «Идентификации и аутентификация. Общие положения» и проекта ГОСТ Р ХХХ-2020 «Идентификации и аутентификация. Уровни доверия к результатам идентификации», в конкретных технических решениях, используемых в ряде ведомств при проектировании, создании и модернизации промышленных систем идентификации и аутентификации, что позволяет, согласно актам об их внедрении, 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 безопасности, связанных с идентификацией и аутентификацией, на 15-30%.

Достоверность и обоснованность результатов диссертации, научных положений и основных выводов работы обеспечена многосторонним анализом современного состояния исследований в предметной области, системным обоснованием предложенных методов, моделей и алгоритмов,

не противоречащих известным положениям теории и практики в области защиты информации, достаточной апробацией основных положений диссертации в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, а также подтверждается в 19 актах о внедрении в различных организациях.

Результаты диссертационных исследований нашли отражение в 67 опубликованных работах в изданиях, рекомендованных ВАК Министерства образования и науки Российской Федерации для публикаций научных результатов докторских диссертаций, в соавторстве опубликовано 3 монографии и 3 учебных пособия.

Апробация результатов работы. Результаты работы докладывались и обсуждались более чем на 85 научных конференциях, трех международных форумах, на которых автором сделано более 300 докладов по теме диссертации.

Автореферат объективно и полно отражает содержание и результаты диссертационной работы, оформлен в соответствии с требованиями «Положения о присуждении учёных степеней» и ГОСТ Р 7.0.11-2011.

Вместе с тем диссертационная работа содержит ряд недостатков, к основным из которых необходимо отнести следующие:

1 в диссертации не показано, что должны включать в себя методологии формирования иерархии уровней доверия к результатам идентификации (раздел 2) и к результатам аутентификации (раздел 3) субъектов доступа, насколько полно эти методологии позволяют решать проблему научно обоснованного формирования иерархии уровней доверия. При этом, если для идентификации в диссертации приведена иллюстрация, в какой-то мере отражающая некоторые подлежащие разработке (или разработанные) в диссертации методы, модели, алгоритмы, процедуры (рисунок 2.2), то применительно к аутентификации такая иллюстрация отсутствует, а в тексте каких-либо пояснений по этому поводу нет. В результате, во-первых, по тексту вдруг возникают подразделы, касающиеся, например, «Методики оценки высокоуровневых рисков аутентификации», «Моделирование процесса аутентификации…», «Концепция моделирования СИА», «Моделирование

протоколов аутентификации» и т.д. Во-вторых, не видно, какой состав моделей и методик требуется иметь для решения проблемы, насколько полно такой комплекс моделей и методик разработан автором и достигнута ли сформулированная им цель работы;

2 в диссертации несколько поверхностно описаны формальные модели и алгоритмы обоснования предлагаемых автором уровней доверия, не показано, как связываются обобщенная функция доверия и входящие в ее определение показатели (см. раздел 3.8) с самими уровнями доверия (см. раздел 3.9). Это снижает, на мой взгляд, теоретическую значимость полученных результатов;

3 в работе имеют место редакционные недостатки, к которым относятся, например, следующие:

по тексту работы автором дается определение понятия «методология формирования иерархии уровней доверия к результатам идентификации субъектов доступа», под которой понимается «совокупность методов и способов реализации» действий, направленных на достижение основной цели – формирования иерархии уровней доверия к результатам идентификации субъектов доступа. Однако из последующего описания не видно, каким образом автор различает между собой методы и способы, почему в схеме, характеризующей данную методологию, способов вообще нет, почему нет в таком определении формальных (математических) моделей. Аналогичным образом, по-видимому, автор понимает и методологию формирования иерархии уровней доверия к результатам аутентификации;

в тексте работы автор сбивается с диссертационного стиля на стиль монографии или пособия, поскольку практически не акцентирует внимание на новизне излагаемого материала и полученных результатов, их отличии от результатов других авторов.

Вместе с тем указанные замечания не меняют общей положительной оценки представленной диссертации.

Вывод. Диссертация Сабанова А.Г. представляет собой законченную научно-квалификационную работу, в которой решена актуальная научная проблема разработки теоретической и методологической базы построения

иерархии доверия к результатам идентификации и аутентификации субъектов доступа, имеющей важное хозяйственное значение. Диссертация написана единолично, содержит совокупность новых научных результатов и положений, имеет внутреннее единство и соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». По актуальности, форме и содержанию, полноте поставленных и решенных задач, совокупности новых научных результатов диссертация соответствует критериям, установленным «Положением о присуждении учёных степеней» для диссертаций на соискание ученой степени доктора наук, а ее автор – Сабанов Алексей Геннадьевич, заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
главный научный сотрудник управления
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
доктор технических наук, профессор Язов
Юрий Константинович

«10» сентября 2020 г.

Подпись Язова Ю.К. заверяю.

Ученый секретарь
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
кандидат технических наук,
старший научный сотрудник Паринов
Игорь Васильевич

«10» сентября 2020 г.

Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)
Почтовый адрес: 394020, г. Воронеж, ул. 9 Января, д. 280А
Тел.:8(473) 257-92-58
e-mail: gniii@fstec.ru