Экз. № __

УТВЕРЖДАЮ
Заместитель начальника академии
по учебной и научной работе
Академии ФСО России
докт. соц. наук., профессор
Козачок Василий Иванович
_____
«20» 10 2020 г.

# ОТЗЫВ

ведущей организации на диссертацию 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 темы диссертации*

Диссертационное исследование А.Г. Сабанова посвящено формированию доверия к результатам идентификации и аутентификации субъектов доступа информационных систем. В современных условиях развития цифровизации тема является актуальной.

*Новизна полученных результатов и выводов*

Согласно содержанию диссертации новизна работы 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 последовательных связанных процедур, что позволило определять вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в корпоративных и открытых информационных системах;
- 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 информационных систем, отличающаяся от известных полнотой выбора критериев, что обеспечило возможность многоуровневого анализа рисков процессов и транзакций в системах идентификации и аутентификации, позволяющих 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.

По нашему мнению, изложенное соответствует требованиям к научной новизне согласно п. 9 Положения ВАК о присуждении ученых степеней, утвержденного Постановлением Правительства РФ № 842 от 24.09.2013 г. в редакции от 02.08.2016 года.

*Апробация работы и публикации*

Результаты исследования докладывались на межотраслевых научных конференциях, проводившихся на базе Академии ФСО России в 2015, 2016 и 2019 годах, по итогам которых было опубликовано 5 работ, из них 2 в соавторстве Сабанова А.Г. с сотрудниками Академии ФСО России. Кроме этого, доклады Сабанова А.Г. слушались и обсуждались на научно-технических конференциях «Методы и технические средства обеспечения информационной безопасности» г. Санкт-Петербург в 2003-2019 гг., научно-практических конференциях, проводимых УМО по специальности «Защита информации», а также конференциях «Комплексная защита информации», 2005-2013 гг., ежегодных научных конференциях по радиофизике Н. Новгород, ННГУ им. Н. И. Лобачевского – 2012 и 2013 гг., международных конференциях «Рускрипто» в 2004-2019 гг., международных конференциях «Инфофорум» - в 2005-2016 гг., международных конференциях "PKI-форум" (СПб) в 2003-2019 гг., Уральском Форуме «Информационная безопасность банков» в 2009-2020 гг., Расширенных заседаниях Совета по обеспечению информационной безопасности таможенных органов РФ в 2006-2015 гг., региональном семинаре Международного союза электросвязи (ITU) в 2013 г., конференциях Международной академии связи в 2013-2019 гг., Международных научно-практических конференциях «ГЛОНАСС-регионам», г. Орёл в 2014-2015 гг., Европейском международном форуме по проблемам электронной подписи. EFPE Польша. Медзыздрое. 4-6 июня 2014 г., Совещании-семинаре работников центрального аппарата и

территориальных органов ФНС России по вопросу информационной безопасности в 2007-2016 гг., VII Международном IT-форуме с участием стран БРИКС и ШОС. Ханты-Мансийск, 6-7 июля 2015 г. и др.

По теме диссертации опубликовано 69 статей в изданиях, рекомендованных ВАК при Минобрнауки России, из них 50 работ без соавторов.

*Обоснованность научных положений и выводов, сформулированных в диссертации*

Научные положения и выводы, приведенные в диссертационной работе Сабанова А.Г. представляются достаточно обоснованными, поскольку опираются как на развитие теории защиты информации в части идентификации и аутентификации, непротиворечащие известным результатам, так и на многочисленные проекты по реализации части представленных в диссертации результатов, подтверждаемых 19 актами о внедрении. Автор достаточно корректно использует известные научные методы обоснования полученных результатов, выводов и рекомендаций. В работе изучены и критически проанализированы известные достижения и теоретические положения других авторов по вопросам исследования и моделирования процессов идентификации и аутентификации.

*Краткий анализ содержания работы*

Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и двух приложений.
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* доказана необходимость проведения системного исследования системы идентификации и аутентификации, а также анализа процессов и процедур, составляющих функционал систем идентификации и аутентификации. Установлена необходимость введения уровней доверия к результатам идентификации и аутентификации, применение которых может повысить надежность и безопасность управления доступом пользователей. Автор показал, что в качестве показателей доверия могут выступать достоверность идентификационной информации, функциональная надежность работы системы, безопасность идентификационной и аутентификационной информации. Установлено, что в качестве основного инструмента для проведения данного исследования должны лежать методы анализа рисками.

Во *второй главе* сформулирована общая методология и подробно рассмотрена задача идентификации субъектов доступа. Установлена зависимость необходимого количества применяемых идентификаторов с известными оценками безошибочности идентификации от числа зарегистрированных в информационных системах субъектов доступа. Предложены модели и разработана методика оценки надежности идентификации. Приведены методы оценки надежности первичной идентификации, а также оценки ошибок идентификационной информации и ошибок при верификации, а также при передаче идентификационной информации. 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 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.

Впервые проведена оценка рисков первичной идентификации. 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 информационных систем 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. Представленные в главе научные результаты позволяют сделать вывод о создании методологии формирования иерархии доверия к результатам идентификации.

*В третьей главе* диссертации рассмотрена проблема оценки доверия к результатам аутентификации субъектов доступа. Выполнен анализ типовых систем идентификации и аутентификации для закрытых корпоративных систем и информационных систем общего пользования с целью выявления типовых особенностей их функционирования для последующего моделирования. Разработана классификация систем идентификации и аутентификации по критериям выполнения целей обеспечения доступности, целостности и конфиденциальности. Установлено, что в целях обеспечения доступности, достоверности результатов и отказоустойчивости на этапах проектирования и совершенствования системы управления должны исследоваться с помощью методов теории массового обслуживания, теории функциональной надежности и теории защиты информации.

Рассмотрены основные информационные потоки и участники процессов идентификации и аутентификации пользователей при удаленном электронном взаимодействии, в том числе при переходе к облачным вычислениям. 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.

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 впервые 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.

В *четвертой главе* показаны возможности применения основных положений данной работы к различным теоретическим и практическим задачам.

В частности, 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. Установлено, что минимально необходимым, и достаточным для большинства операций с электронными документами, является следующий набор сервисов безопасности:

- аутентификация (ГОСТ Р 58833 – 2020, ISO 29115: 2013);
- электронная подпись (ГОСТ Р 34.10-2012, ISO/IEC 13888-1);
- метка доверенного времени (RFC 3161 «Time-Stamp Protocol (TSP)»;
- валидация сертификата ключа проверки подписи (RFC 2459);
- проверка полномочий подписанта (ITU-T X.509, v.7);
- доверенная гарантированная доставка документов и сообщений.

Использование совокупности указанных сервисов позволит повысить уровень доверия к электронному документу до уровня официальных бумажных документов, что необходимо для развития цифрового общества и цифровой экономики.

Из заключения, приведенного автором диссертационной работы, следует отметить следующие важные на наш взгляд 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 информационной системе. 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 информационных системах с большим числом субъектов доступа.

3) Разработан метод оценки рисков первичной идентификации для корпоративных информационных систем и систем открытого типа с личной явкой субъекта к регистратору и в удаленном режиме, без личной явки. Приведены оценки рисков для указанных типов информационных систем. 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 информационных систем 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 решен ряд практических задач, позволяющих существенно повысить уровень защищенности 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.

*Соответствие содержания диссертации автореферату и указанной специальности*

Автореферат соответствует содержанию диссертационной работы и отражает ее основные положения. Также основные положения диссертации нашли отражение в публикациях автора, в том числе в трех монографиях.

*Достоверность*

Выводы и результаты, полученные диссертантом, обоснованы и достоверны, поскольку они опираются на существующую теоретико-методологическую и нормативно-правовую базу и подтверждаются отсутствием противоречий полученных результатов с известными положениям других авторов, а также положительным эффектом от внедрения в практику построения и модернизации систем идентификации и аутентификации в организациях различного подчинения.

*Значимость результатов для науки и производства*

Результаты работы вносят существенный вклад в развитие научных знаний по проблеме доверия к результатам идентификации и аутентификации, без решения которой невозможно успешное построение цифровой экономики и цифрового взаимодействия, полностью заменяющего традиционный бумажный документооборот по доверию к адресатам и подписантам сообщений и документов.

Результаты диссертационного исследования рекомендуются к использованию при проектировании и модернизации систем идентификации и аутентификации современных информационных систем.

*Замечания по диссертационной работе*

1. Некоторые разделы диссертации, особенно в главе 1, носят описательный характер. Часть текста можно было бы сократить без особого ущерба научному содержанию.
2. В таблице 4 автореферата (таблица 3.10 диссертационной работы) в правой нижней ячейке стоит обозначение «самый высокий» (уровень доверия к результату аутентификации). На наш взгляд, это не самая удачная градация. Технологии не стоят на месте. Возможно, следовало бы использовать количественный эквивалент шкалы для обеспечения возможности ее соотнесения с новыми технология аутентификации и идентификации.
3. По тексту работы не совсем понятно, можно ли перейти от принятой в диссертации качественной шкалы уровней доверия (низкий, средний, высокий, ...) к количественному уровню? Тогда критерии доверия к результатам аутентификации и идентификации можно было бы выразить оценивать более точно.
4. Пункт 8 заключения автореферата содержит цифровые выражения в процентах, показывающие преимущества от внедрения результатов

диссертационной работы, которые по тексту диссертации, а также в выводах по главам и в заключении ранее не упоминались (например, снижение затрат на администрирование систем управления доступом на 25-40%). При внимательном изучении диссертационной работы можно убедиться, что данные получены из актов о внедрении, приведенных в Приложении 2 диссертации. В качестве пожелания, указанные цифры было бы логично привести в тексте диссертационной работы.

5. Текст диссертации и автореферата изобилует введенными автором аббревиатурами (некоторые из которых использовались не более двух раз), что затрудняет восприятие представленных результатов.

Отмеченные недостатки снижают качество исследования, но они не влияют на главные теоретические и практические результаты диссертации.

*Выводы*

Диссертационная работа Сабанова Алексея Геннадьевича «Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа» является научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны теоретические положения, совокупность которых можно квалифицировать как решение научной проблемы, имеющей важное социально-экономическое и хозяйственное значение, и удовлетворяет критериям пунктов 9-14 Положения о присуждении ученых степеней, утвержденного постановлением Правительства РФ от 24 сентября 2013 года № 842 (ред. от 02.08.2016), предъявляемым к диссертациям на соискание ученой степени доктора наук, а ее автор заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв подготовлен сотрудниками Академии ФСО России: доктором технических наук А.В. Козачком и кандидатом технических наук, доцентом А.Н. Цибулей.

Отзыв рассмотрен и одобрен на заседании кафедры «Безопасности сетевых технологий» федерального государственного казенного военного образовательного учреждения высшего образования «Академия Федеральной службы охраны Российской Федерации», протокол № 11 от «22» октября 2020 года.

**Сведения о ведущей организации:** Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России, г. Орёл)

Адрес: Приборостроительная ул., 35, Орёл 302015
Тел.: (4862) 54-99-33
Электронная почта: sec@academ.msk.rsnet.ru
Сайт: academ.msk.rsnet.ru

Сотрудник Академии ФСО России
доктор технических наук  Козачок Александр Васильевич

Сотрудник Академии ФСО России
кандидат технических наук, доцент  Цибуля Алексей Николаевич

Спирин Андрей Андреевич
8-4862-54-99-33