

ОТЗЫВ

на автореферат диссертации САБАНОВА Алексея Геннадьевича
**«Методология формирования иерархии доверия к результатам
идентификации и аутентификации субъектов доступа»,**
представленной на соискание учёной степени доктора технических наук
по специальности **05.13.19 – Методы и системы защиты информации,
информационная безопасность**

Актуальность работы Сабанова А.Г. объясняется необходимостью разрешения *проблемной ситуации*, состоящей в противоречии между ростом угроз информационной безопасности, ограниченностью известных моделей и методов управления доступом пользователей, и необходимостью обеспечения требуемой кибербезопасности современных цифровых платформ и экосистем.

Актуальность работы подтверждается требованиями следующих документов:

- Национальная программа «Цифровая экономика Российской Федерации» от 26 июля 2017 года, мероприятия 05.01.001.001.001 и 05.01.002.01.002;

- «Доктрина информационной безопасности Российской Федерации», утв. Указом Президента Российской Федерации от 5 декабря 2016 г. №646;

- ФЗ-187 от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах...» и пр.

Таким образом, тема диссертационной работы Сабанова А.Г. является своевременной и актуальной, а решаемая научная проблема *«Создание методологии формирования иерархии доверия к результатам идентификации и аутентификации субъектов и объектов доступа на основе адаптивного прогнозирования и самоорганизации»* имеет важное теоретическое и практическое значение.

К основным научным результатам, определяющим значимость и новизну диссертационной работы Сабанова А.Г. относятся:

1. Предложена методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа в условиях роста угроз безопасности. Существенно, что упомянутая методология основана на риск-ориентированном подходе и учитывает специфику процессов идентификации и аутентификации.

2. Выработан способ многоуровневой оценки рисков на основе разбиения процесса аутентификации на ряд последовательных связанных процедур, что позволило определить вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в современных цифровых платформах и системах.

3. Создана система классификации методов, алгоритмов и средств идентификации и аутентификации с доказательствами полноты, разрешимости и непротиворечивости.

4. Разработан комплекс моделей и методов оценивания рисков первичной идентификации субъектов доступа на основе матриц рисков к первичной идентификации, что позволило определить величины допустимых рисков и средних значений рисков вероятных опасных событий в условиях в условиях роста угроз безопасности.

5. Предложена методика для оценивания структурно-функциональной надежности процессов идентификации и аутентификации, отличающаяся возможностями адаптивного прогнозирования и самоорганизации.

Основные научные результаты диссертационной работы, выносимые на защиту, получены лично автором, что подтверждается их использованием при подготовке работы, многократными выступлениями на российских и зарубежных научно-технических конференциях, участием в выполнении тематических НИР, а также использованием результатов в научно-педагогической деятельности.

Полученные результаты нашли свое отражение в следующих государственных контрактах и НИР (НИОКР):

- ФСТЭК России, шифр работ «Момент-16», 2016 г., «Идентификация», 2018 г.;
- Министерстве науки и образования, шифр работы (темы) 14.577.21.0172 от 01.11.2015;
- Министерстве коммуникаций и связи РФ, гос. контракт № 012/155 от 12.12.2011;
- ФТС России (9 гос. контрактов 2007–2011 гг.);
- Пенсионном фонде РФ (гос. контракты № 14-141-D от 18.05.2009, № 23-158-D от 04.05.2010 и др. – всего 9 гос. контрактов);
- В ряде инициативных НИР по созданию перспективных средств защиты информации JaCarta, JaCarta SF/ГОСТ, Secret Disk Enterprise, JaCarta Management System, СКЗИ «КриптоБД» и др.

По теме диссертационной работы автором исследования подготовлено 67 работ, в том числе 50 публикаций в изданиях, рекомендованных ВАК РФ, две статьи в изданиях, цитируемых в Web of Science, получены два патента на изобретение: № 2523174 от 22.05.2014 (соавтор) и № 2635927 от 5.09.2016 (соавтор), в соавторстве опубликованы 3 монографии, 3 учебных пособия, из них два с грифом УМО.

Автореферат диссертации Сабанова А.Г. написан четким, лаконичным языком, достаточно подробно иллюстрирован, полностью соответствует содержанию диссертации и даёт целостное представление о поставленных задачах и достигнутых результатах.

Тема диссертации, направленность выполненных исследований и полученных результатов соответствует специальности 05.13.19 – «Методы и

системы защиты информации, информационная безопасность» по п. 1 (теория и методология обеспечения информационной безопасности и защиты информации); п. 3 (методы и модели выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса); п. 6 (модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования); п. 9 (модели и методы оценки защищенности информации и информационной безопасности объекта).

Имеется ряд замечаний:

1. Методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа в условиях роста угроз безопасности основывается на риск-ориентированном подходе и учитывает специфику процессов идентификации и аутентификации. При этом из автореферата не совсем ясно, каким образом проводилась оценка трудоемкости и достоверности предложенных моделей и методов количественного оценивания рисков. Являются ли предлагаемые метрики и меры для оценивания рисков достаточными?

2. В настоящее время осуществляется переход от Концепции обеспечения кибербезопасности к более широкой Концепции киберустойчивости критически важной информационной инфраструктуры Российской Федерации. Новая Концепция подразумевает гарантированное достижение поставленных целей и задач в условиях как известных, так неизвестных угроз безопасности. Какие новые требования к моделям и методам идентификации и аутентификации субъектов доступа здесь появляются? Как будут соотноситься такие понятия как кибербезопасность (и контроль доступа в частности), функциональная надежность и отказоустойчивость с понятиями структурно-функциональной устойчивости, живучести и киберустойчивости цифровых систем и платформ.

4. Требуется пояснить, какие изменения последуют в предлагаемых моделях и методах идентификации и аутентификации в случае перехода с традиционной архитектуры фон Неймана на новые архитектуры квантовых когноморфных, иммунных и нейронных компьютеров. Какие изменения придется вносить в предлагаемую методику оценивания структурно-функциональной надежности процессов идентификации и аутентификации.

3. Из автореферата не совсем ясно достаточно ли для обеспечения высокого уровня надежности аутентификации: хранения контейнеров ключевого материала в защищенном от копирования чипе; применения SSCD (Secure Signature Creation Device). Или потребуются дополнительные контрмеры (если да, то какие).

5. Следовало бы уточнить, может ли представленный подход и разработанная методология построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа стать научно-

технической и методической базой для разработки нормативных требований к созданию высоконадежных систем аутентификации.

Вместе с тем, указанные недостатки в целом не влияют на высокую оценку научного уровня проведенных исследований и позволяют сделать положительный вывод о качестве результатов, представленных в автореферате и диссертации.

Выводы:

Диссертационная работа Сабанова А.С. написана на актуальную тему, отличается научной новизной, теоретической и практической значимостью, прикладной ценностью полученных результатов, выполнена лично соискателем и имеет завершённый характер.

Сабановым А.С. сформулирована и решена актуальная и масштабная научная проблема, значимая для обеспечения информационной безопасности Российской Федерации и заключающаяся в *создании методологии формирования иерархии доверия к результатам идентификации и аутентификации субъектов и объектов доступа на основе адаптивного прогнозирования и самоорганизации.*

Диссертационная работа соответствует критериям пунктов (п.п. 9-14) «Положения о присуждении учёных степеней», утверждённым постановлением Правительства РФ от 24.09.2013 г. № 842, предъявляемым к диссертациям на соискание ученой степени доктора наук, а её автор, Сабанов Алексей Геннадьевич, заслуживает присуждения учёной степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Руководитель Центра информационной безопасности
АНО ВО «Университет Иннополис»,
эксперт секции по проблемам информационной безопасности
научного совета при Совете Безопасности
Российской Федерации,
доктор технических наук, профессор

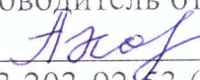


Петренко Сергей Анатольевич

420107, Республика Татарстан, г. Иннополис,
ул. Университетская, д. 1
тел.: 8 (903) 742-85-43
e-mail: s.petrenko@innopolis.ru

15.10.2020 г.

Подпись профессора Петренко С.А. удостоверяю

Руководитель отдела по работе с персоналом

Ахунова Эльвира Рубисовна
+7 843 203-92-53 (120) e.akhunova@innopolis.ru