УТВЕРЖДАЮ

Проректор по НРиИ

_____ А.Г. Лощилов

«___» июня 2020 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Диссертация «Методология формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа» выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС).

В период подготовки диссертации соискатель Сабанов Алексей Геннадьевич обучался в докторантуре в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» на кафедре комплексной информационной безопасности электронно-вычислительных систем.

Во время обучения в докторантуре Сабанов А.Г. совмещал научную и педагогическую деятельность. В настоящее время он работает в должности инженера кафедры комплексной информационной безопасности электронно-вычислительных систем и доцента кафедры ИУ-10 МГТУ им. Н.Э. Баумана.

В 1980 году окончил факультет аэромеханики и летательной техники Московского физико-технического института (МФТИ) по специальности «Летательные аппараты». С 1983г. по 1987г. обучался в аспирантуре МФТИ, которую закончил с предоставлением кандидатской диссертации. Диплом кандидата технических наук: серия ТН №112900, Москва, 21сентября 1988г., выдан решением диссертационного совета в Московском физико-техническом институте от 14 апреля 1988г., протокол №24.

Научный консультант – Шелупанов Александр Александрович, доктор технических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники», ректор.

По итогам обсуждения принято следующее заключение:

Оценка выполненной соискателем работы.

Диссертация Сабанова А.Г. является законченной научно-квалифицированной работой, в которой решена актуальная научно-техническая проблема создания теоретической и методологической базы построения иерархии доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии.

Актуальность темы и направленность исследования.

Основной целью системы управления доступом информационной системы (ИС) является принятие обоснованного положительного или отрицательного решения по запросу на авторизацию. В условиях недостатка общепринятых научных взглядов, нормативных требований и методических рекомендаций уполномоченных государственных органов операторы ИС самостоятельно выбирают механизмы и средства идентификации и аутентификации (ИА), что повышает риски реализации атак, направленных на предоставление доступа злоумышленнику. В связи с интенсивной цифровизацией практически всех сфер деятельности граждан проблема доверия к результатам ИА субъектов доступа в ИС различного назначения становится весьма актуальной. Ключевой проблемой является отсутствие общепринятых походов к оценке рисков, связанных с ИА, способов построения иерархии доверия к результатам ИА на основе анализа рисков и критериев оценки доверия к результатам ИА.

Личное участие автора в получении результатов.

В диссертации использованы результаты, в которых автору принадлежит основная роль в постановке, решении научных задач и в общении полученных результатов. Без соавторства опубликовано 30 основных работ. Некоторые из публикаций написаны в соавторстве с сотрудниками КИБЭВС ТУСУР, МГТУ им. Н.Э. Баумана, НИИАС РЖД, ИСА РАН, ЗАО «Аладдин Р.Д.». В совместных публикациях автору принадлежит постановочная часть, участие в проведении исследований и интерпретации результатов. В реализации проектов и выполненных НИР, как правило, автор являлся научным руководителем работ.

Степень достоверности результатов диссертации.

Достоверность изложенных в работе результатов обеспечивается многосторонним анализом современного состояния исследований в предметной области, теоретическим обоснованием предложенных методов, моделей и алгоритмов, не противоречащих известным положениям других авторов, 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 в практику построения и модернизации систем идентификации и аутентификации в организациях различного подчинения, о чем свидетельствуют соответствующие акты о внедрении.

Научная новизна диссертации.

Научная новизна результатов работы и проведенных исследований 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,

отличающиеся от известных учетом анализа рисков и специфики процессов идентификации и аутентификации, в том числе для больших информационных систем с числом пользователей порядка 10^6 с учетом перехода к облачным вычислениям;

- разработан метод оценки рисков первичной идентификации субъектов доступа с помощью матриц рисков, отличающийся от известных применением динамического метода построения матриц рисков к первичной идентификации, который позволяет определять значения допустимых рисков и средних значений рисков вероятных опасных событий;
- предложен способ многоуровневой оценки рисков и исследования надёжности на основе разбиения процесса аутентификации на ряд последовательных процедур, отличающийся от известных комплексным подходом и практической направленностью, что позволило определять вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в корпоративных и открытых ИС;
- проведена оригинальная классификация методов и систем идентификации и аутентификации, а также средств и механизмов аутентификации для выявления границ применимости различных технологий ИА 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 проводить оценки рисков с заданным уровнем детализации;
- разработаны вероятностно-статистические математические модели и методики оценки надёжности процессов идентификации и аутентификации, отличающиеся от известных тем, что оценивался не отказ оборудования, а отказ услуг, что в соответствии с многоуровневым принципом исследования позволяет проводить оценку функциональной надежности как системы идентификации и аутентификации целиком, так и выполняемых процессов, а также отдельных процедур, таких как первичная идентификация участников удалённого электронного взаимодействия.

Практическая значимость диссертации.

Практическая значимость полученных результатов заключается в том, что в диссертации решена важная проблема разработки методологии формирования иерархии уровней доверия и оценки доверия к результатам идентификации и аутентификации субъектов доступа, позволяющая использовать ее в практической деятельности по построению и модернизации систем управления доступом современных информационных систем, что подтверждается актами о внедрении 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 информационных систем различного назначения, как минимум, на 25%.

Прикладная направленность диссертационной работы проявилась в разработке национальных стандартов, научно-технических отчетов, конкретных технических решениях, используемых в ряде ведомств. Так, результаты диссертационного исследования использовались при разработке ГОСТ Р 58833 «Защита информации. Идентификация и аутентификация. Общие положения», проекта ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия к результатам идентификации», проектировании, создании и модернизации промышленных систем идентификации и

аутентификации, что подтверждено соответствующими актами об использовании результатов диссертационного исследования.

Полнота изложенных материалов диссертации в печатных работах, опубликованных автором.

По материалам диссертации Сабанов А.Г. опубликовал 67 публикаций (из которых 50 без соавторов) в изданиях, рекомендованных ВАК России, две статьи в изданиях Web of Science, два патента на изобретение №2523174 от 22.05.2014 г.(соавтор) и №2635927 от 05.09.2016 г.(соавтор), в соавторстве опубликовано 3 монографии, 3 учебных пособия, из них два с грифом УМО.

Статьи в журналах, рекомендованных ВАК при Минобрнауки России:

1. Сабанов А.Г. Аутентификация как часть единого пространства доверия // Электросвязь. 2012. №8. С.40-44.
2. Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь. 2013. №4. С.27-32.
3. Сабанов А.Г. Основные процессы аутентификации // Вопросы защиты информации. 2012. №3. С.54-57.
4. Сабанов А.Г. Особенности аутентификации при доступе к облачным сервисам // Вестник Нижегородского университета им. Н.И. Лобачевского. 2013. №2-1. С.45-51.
5. Сабанов А.Г. Методы исследования надежности удаленной аутентификации // Электросвязь. 2012. №10. С.20-24.
6. Сабанов А.Г. Об уровнях строгости аутентификации. // Доклады ТУСУР. 2012. №2(26). С.134-139.
7. Сабанов А.Г. Комплексная защита электронного документооборота // Оборонный комплекс научно-техническому прогрессу России. 2012. № 4. С.72-77.
8. Додохов А.Л., Сабанов А.Г. Способ защиты баз данных, содержащих персональные данные // Вопросы защиты информации. 2013. №3. С.4-9.
9. Сабанов А.Г. Модели для исследования безопасности и надежности процессов аутентификации // Электросвязь. 2013. №10. С.38-42.
10. Сабанов А.Г. Классификация процессов аутентификации // Вопросы защиты информации. 2013. №3 С.46-52.
11. Додохов А.Л., Сабанов А.Г. Один из подходов к защите персональных данных в публичных облачных приложения // Вопросы защиты информации. 2013. №2 (101). С.3-9.
12. Сабанов А.Г. Концепция электронного пропуска сотрудника предприятия оборонно-промышленного комплекса // Оборонный комплекс научно-техническому прогрессу России. 2013. № 3. С.10-16.
13. Сабанов А.Г. Вопросы идентификации и аутентификации в информационных системах общего использования // Информационно-измерительные и управляющие системы. 2013. т.11., №7. С. 81-84.
14. Сабанов А.Г. Аутентификация при электронном обмене конфиденциальными документами // Доклады ТУСУР. 2011. №2(24). С.263-266.
15. Додохов А.Л., Сабанов А.Г. Исследование применения СУБД Oracle для защиты персональных данных // Доклады ТУСУР. 2011. №2(24). С.267-270.
16. Сабанов А.Г. Концепция моделирования процессов аутентификации //Доклады ТУСУР. 2013 №3(29). С.71-75.

17. Сабанов А.Г. Методика идентификации рисков процессов аутентификации. Доклады ТУСУР. 2013. №4 (30), С. 93-97.
18. Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности // Электросвязь. 2014. №2 (113). С.6-9.
19. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации // Вопросы защиты информации. 2014. №1(104). С.13-22.
20. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь 2014. №5. С.44-47.
21. Сабанов А.Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии. // Доклады ТУСУР, 2014. №2(32). С.180-184.
22. Сабанов А.Г. О применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь 2014. №6. С.39-42.
23. Сабанов А.Г., Смолина С.Г. Сравнительный анализ биометрических методов идентификации личности // Труды ИСА РАН. 2016. Том 66 3/2016. С.12-21.
24. Сабанов А.Г. О формировании уровней доверия к идентификации и аутентификации субъектов при удаленном электронном взаимодействии // Электросвязь. 2015. №10. С.46-51.
25. Сабанов А.Г. О неизвлекаемости закрытых ключей // Инсайд. Защита информации. 2015. №2. С.30-33.
26. Сабанов А.Г. Доверенные системы как средство противодействия кибер-угрозам. // Инсайд. Защита информации. 2015. №3. С.17-21.
27. Сабанов А.Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 1 // Инсайд. Защита информации. Часть 1. 2016. №2(68). С.84-87. / Часть 2. 2016. №3. С.70-74.
28. Сабанов А.Г. О доверии к сервисам безопасности, обеспечивающим юридическую силу электронным документам // Первая миля. 2016. №1 (#54). С.42-43 (часть 1). №2 (#55). С.34-37 (часть 2).
29. Сабанов А.Г. Об уровнях аутентификации в информационном обществе // Инсайд. Защита информации. 2012. № 2(44). С.68-74.
30. A. Sabanov. Information Security Aspects in e-Commerce. APEC Conference 15-16 November, 2008. Pekin, Chine.pp.78-83.
31. Сабанов А.Г. Биометрическая идентификация: оправдаются ли ожидания? // Первая миля. 2014. №1(#40). С.59-60.
32. Сабанов А.Г. Юридическая сила электронного документа: технологическая составляющая // Инсайд. Защита информации. 2014. №3. С.20-25.
33. Сабанов А.Г. Способ определения строгости аутентификации // Электросвязь. 2016. №8. С.56-61.
34. Сабанов А.Г. Некоторые проблемы доверия к электронному документу // Инсайд. Защита информации. 2018. №3(79). С.10-15.
35. Минаев В.А., Королев И.Д., Сабанов А.Г. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия // Вестник УрФО. Безопасность в информационной сфере. 2018. №3(30). С.43-49.

36. Сабанов А.Г. Критерии доверия к результатам идентификации субъектов доступа // Электросвязь. 2019. №3. С.38-44.
37. Сабанов А.Г. Уровни доверия к аутентификаторам // Вопросы защиты информации. 2019. №2. С.10-17.
38. Сабанов А.Г. Вопросы доверия к результатам аутентификации субъекта доступа // Методы и технические средства обеспечения безопасности информации» №28. СПб. 2019. С.57-59.
39. Сабанов А.Г. Уровни доверия к результатам идентификации и аутентификации субъекта доступа в период цифровой трансформации // Вопросы кибербезопасности. 2019. №5 (33). С.19-25.
40. Mark Mamchenko, Alexey Sabanov. Exploring the Taxonomy of USB-Based Attacks // 2019 Twelfth International Conference "Management of large-scale system development" (MLSD) pp. 926-929 / IEEE *Xplore*: 25 November 2019// DOI: 10.1109/MLSD.2019.8910969 https://ieeexplore.ieee.org/document/8910969.
41. Сабанов А.Г. Концепция предварительного анализа рисков первичной идентификации субъектов доступа // Инсайд. Защита информации. 2020. № 2. С.74-79.
42. Сабанов А.Г., Шубинский И.Б. Метод анализа технологических рисков первичной идентификации субъектов доступа// Инсайд. Защита информации. 2020. № 3. С.57-61.
43. Сабанов А.Г. Моделирование процесса первичной идентификации субъектов доступа для оценки достоверности автоматической регистрации // Инсайд. Защита информации. 2020. № 4 (в печати).

Монографии:

44. Национальная платежная система. Бизнес-энциклопедия» / коллектив Н35 авторов [В.В. Адрианов, М.Я. Букирь,… Сабанов А.Г.,…]; ред.-сост. А.С. Воронин. – М.: КНОРУС : ЦИПСиР, 2013. – 424с.
45. Бизнес-энциклопедия «Платежные карты» / И.М. Голдовский, М.Ю. Гончарова, А.Н. Грачев,…А.Г. Сабанов,… ред.: А.С. Воронин .— 2-е изд., перераб. и доп. — М. : КНОРУС : ЦИПСиР, 2014. — 558 с. [Электронный ресурс] Режим доступа: https://rucont.ru/efd/364245.
46. Сабанов А.Г., Зыков В.Д., Мещеряков Р.В.,Рылов С.П., Шелупанов А.А. «Защита персональных данных в медицинских организациях». М.: Горячая линия - Телеком, 2011. 205с.

Учебные пособия:

47. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А., Газизова Э.Р., Додохов А.Л., Крячков А.В., Кузнецов С.Б., Полянская О.Ю., Сабанов А.Г., Скида М.А., Халяпин С.Н. Аутентификация. Теория и практика. Под ред. Проф., д.т.н. Шелупанова. М.: Горячая линия-Телеком, 2009,- 552с.: ил.
48. Удостоверяющие автоматизированные системы и средства: Введение в теорию и практику удостоверяющих автоматизированных систем: монография/ Н12 авто-ров [С.В. Баушев,…А.Г.Сабанов,…]. Под ред. С.В. Баушева и А.С. Кузьмина. – СПб.: БХВ-Петербург, 2016. – 304с.:ил.
49. Сабанов А.Г. Идентификация и аутентификация пользователей / Ин-формационно-методическое пособие. Издательский дом "Афина". 2018. – 287с.:ил. [Электронный ресурс] Режим доступа: www.inside-zi.ru

Соответствие содержания диссертации избранной специальности

Диссертационная работа Сабанова А.Г. по своему содержанию соответствует профилю специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», в частности, по следующим пунктам:

1. Теория и методология обеспечения информационной безопасности и защиты информации.

2. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.

11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.

Ценность научных работ соискателя, полнота изложения материалов в опубликованных работах.

Представленная работа соответствует требованиям п.9 Положения о присуждении ученой степени доктора технических наук.

В работе решена актуальная научно-техническая проблема разработки методологии формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа существующих и перспективных информационных систем. Практические результаты работы, подтвержденные актами о внедрении, имеют важное социально-экономическое значение для повышения безопасности управления доступом в информационных системах различного назначения.

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

Заключение принято на заседании научно-технического семинара «Интеллектуальные системы моделирования, проектирования и управления» кафедры комплексной информационной безопасности электронно-вычислительных систем факультета безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Присутствовало на заседании 26 чел. Результаты голосования: «за» – 26 чел., «против» – 0 чел., «воздержалось» – 0 чел., протокол № 342 от 30 мая 2020 г.

Зам. председателя семинара,
канд. техн. наук, доцент,
доцент каф. КИБЭВС _____ А.А. Конев

Ученый секретарь семинара,
канд. техн. наук, доцент,
доцент каф. КИБЭВС _____ Е.Ю. Костюченко