Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

107023, г. Москва, ул. Электрозаводская, д. 24, стр. 1, тел.: +7 (495) 223 23 92, факс: +7 (499) 113-45-09, mail@npo-echelon.ru, npo-echelon.ru

Исх. № 2196 от « 9 » 10 2020 г.

Утверждаю
Генеральный директор
АО «НПО «Эшелон»
кандидат технических наук, доцент

В.Л.Цирлов

«9» октября 2020 г.

ОТЗЫВ

на автореферат диссертации

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

I. Актуальность проблематики и темы диссертационного исследования

Актуальность и востребованность работы объясняется потребностью разрешения проблемной ситуации, состоящей в противоречии между высоким уровнем неопределенности оценки процессов аутентификации в развивающейся гиперсложной распределённой открытой среде в условиях тематических кибератак (например, при перехвате и подмене сессий и иной аутентификационной информации, «маскараде», создании клонов, атак на отказ в обслуживании и обход сетевых средств разграничения доступом, атак на облачные вычисления, криптоатак на протоколы аутентификации, атак социальной инженерии, APT-операциях и пр.) и собственно недостаточным

уровнем развития теоретических исследований и разработанности методической базы идентификации и аутентификации субъектов современных информационных систем на фоне новых требований по безопасности информации в киберпространстве.

Указанная проблематика, на наш взгляд, коррелируется с «Основными направлениями научных исследований в области обеспечения ИБ РФ» (Совет Безопасности Российской Федерации, 2017 г.) по пп. 1.1.9 и 2.2.10.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствуют Паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по пп. 1, 11 и др.

II. Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность и новизна

Судя по автореферату, в диссертационном исследовании автор, опираясь на проведенный анализ особенностей открытых развивающихся компьютерных сетей и их подсистем управления доступом, нормативно-правой базы в части аутентификации и управления рисками, таксономий и систематик информационной безопасности, в том числе по уязвимостям, угрозам и атакам на подсистемы и средства аутентификации, инструментальной базы тестирования, контроля и мониторинга защищенности, формальных моделей и методов управления безопасным доступом, а также управления рисками, прикладных пакетов компьютерного моделирования (СМО), демонстрирует системность и комплексность своего подхода к постановке и разрешению научной проблемы.

Оригинальность работы состоит в том, что автор исследовал концептуальные и методические основы идентификации и аутентификации, в рамках чего предложил новые систематики и методы оценки уровня идентификации и аутентификации на основе принципа доказательности безопасности («доверия») и с учетом риск-ориентированного подхода.

Наиболее существенные новые научные результаты, полученные в диссертации, состоят в предложении **нового научно-обоснованного** концептуального подхода, а также методов, математических моделей и методик решения поставленных в диссертации задач. К новым научным

результатам, полученным в диссертационном исследовании, следует отнести следующие:

1. Концептуальные основы построения иерархии доверия к результатам процесса идентификации и аутентификации субъектов (отличающиеся от известных учетом рисков информационной безопасности и факторов процесса аутентификации), позволяющие повысить точность оценки уровня информационной безопасности распределенных систем;

2. Метод матричной оценки рисков первичной идентификации субъектов доступа, позволяющий определять значения допустимых рисков и средние значения рисков вероятных опасных событий в процессе аутентификации;

3. Методика многоуровневой оценки рисков, что позволяет определять вероятностные характеристики разнородных по длительности и повторяемости процедур аутентификации;

4. Таксономия процесса аутентификации, позволяющая повысить полноту решений;

5. Математические (вероятностные) модели расчета степени надежности подсистемы аутентификации, позволяющие повысить точность оценки.

Согласно автореферату (по утверждению автора), представленные научные результаты не имеют аналогов.

Достоверность основных выводов и результатов диссертационного исследования подтверждается тем, что:

- в работе корректно использован аппарат теории вероятности, теории множеств, теории надежности и их теоретические приложения;

- научный замысел базируется на анализе потребностей практики обеспечения безопасности сетей общего доступа;

- представлены проверяемые данные, факты и статистическая информация.

Достоверность, новизна и значимость научных результатов исследования подтверждены 2-мя патентами (на изобретение), материалами НИР и ОКР («Момент-16», «Идентификация» и др.), а также актами о внедрении.

III. Теоретическая значимость и практическая ценность результатов исследований

Теоретическая значимость результатов состоит в создании концептуальных основ теории доверия к процессам аутентификации, а также в развитии методов теория защиты информации в части систематики иерархической идентификации и аутентификации, развитии приложений теории вероятности в части новых моделей аутентификации и др.

Практическая ценность исследования определяется тем, что результаты диссертационного исследования представлены в том числе в виде предложений по нормативно-техническому облику современных и перспективных систем аутентификации. Ряд результатов исследования вошел в инновационный национальный с стандарт ГОСТ Р 58833-2020, а также в ряд проектов стандартов ГОСТ Р «Уровни доверия к результатам идентификации», «Уровни доверия к результам аутентификации» и др. По утверждению автора, применение положений работы «позволяет сократить, как минимум, на 25% сроки проведения оценок безопасности, функциональной надежности и достоверности результатов ИА СД на этапах проектирования и эксплуатации ИС, а также администрирования СИА», что представляется весьма внушительным научно-прокладном результатом для народного хозяйства и безопасности страны.

IV. Характеристика опубликованности результатов и положений, выносимых на защиту

Опубликованность научных результатов диссертационной работы подтверждается 65-ю статьями в рецензируемых журналах, включенных в текущий перечень ВАК (согласно РИНЦ), а также одной научной публикацией, проиндексированной в базе Scopus. Положения работы прошли апробацию на множестве научно-практических конференций и в учебном процессе ряда вузов.

Ознакомление с авторефератом и другими научными трудами автора позволяет сделать однозначный вывод, что диссертация является **единолично** написанной научно-квалификационной работой.

IV. Замечания и недостатки диссертационной работы

Несмотря на научный интерес к исследованию, диссертационная работа, судя по автореферату, не свободна от недостатков и вопросов, к которым, например, могут быть отнесены следующие:

1. В отдельных случаях автор не придерживается общепринятой в информационной безопасности научной терминологии (например, под методологией, как правило, принято понимать организацию деятельности, а уровень доверия обычно ассоциируют с линейкой ISO/IEC 15408), что незначительно затрудняет оценку работы.

2. В автореферате рис.1 («Методология..») представлен мелким шрифтом, что затрудняет оценить сформулированность научной проблемы (как сложноорганизованной системы исследовательских задач принципиального характера, обладающих существенной неопределённостью). При этом, к сожалению, автор не привел формальную постановку проблемы, в том числе несколько лаконично обосновал обобщенный показатель. Это несколько снижает оценку завершенности работы (неясно, как изменился целевой показатель работы).

3. Отдельные приведенные в автореферате формулы, на наш взгляд, имеют незначительные опечатки или некорректности, например, уравнение полной вероятности на с. 19, а также формула (6). Представление (в главах 2-3) вероятностных моделей без оценки их точности (и пр.), а также весьма лаконичное обоснование и описание примера СМО (глава 4) несколько затрудняют оценку значимости 5-го научного результата.

В целом отмеченные недостатки принципиально не снижают научной значимости работы, так как поставленная в работе цель («создание методологии формирования иерархии доверия к результатам ИА субъектов доступа, в том числе при удаленном ЭВ»), судя по автореферату, достигнута. К достоинствам работы необходимо отнести прикладную направленность (в первую очередь в плане подготовки прорывных национальных стандартов), широкий кругозор и опыт автора, актуальность и востребованность, завершенность, безусловную оригинальность и пионерский характер исследований. Автореферат характеризуется логичностью изложения и соответствующим научным стилем написания. Что касается содержания, то, на наш взгляд, работа бы выиграла, если бы автор пять защищаемых научных

результатов представил бы в большем количестве глав, чем в двух. При этом все выносимые положения аргументированы и понятны.

V. Вывод

Таким образом, судя по автореферату и печатным работам, диссертационная работа Сабанова А.Г. представляет собой законченную научно-квалификационную работу, выполненную лично соискателем на актуальную тему, которая отличается научной новизной, теоретической значимостью и прикладной ценностью в области информационной безопасности.

На наш взгляд, автором в диссертации сформулирована и решена **проблема**, состоящая в разработке концептуальных основ и методического аппарата формирования иерархии доверия к результатам идентификации и аутентификации субъектов доступа, имеющая важное значение для обеспечения информационной безопасности сетевых инфраструктур Российской Федерации. В то же время, судя по многочисленным публикациям и внедрениям, а также монографиям и отчетам о НИР, в диссертации разработаны теоретические положения, **совокупность** которых, на наш взгляд, возможно квалифицировать и как научное достижение.

Полагаем, что диссертационная работа соответствует требованиям пункта 9 постановления Правительства Российской Федерации от 24.09.2013 № 842 «О порядке присуждения ученых степеней», а ее автор, Сабанов Алексей Геннадьевич, заслуживает присвоения ему ученой степени доктора технических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Президент Акционерного общества
«Научно-производственное объединение «Эшелон»
доктор технических наук, старший научный сотрудник

Алексей Сергеевич Марков

« 9 » октября 2020 года

Контактная информация: 107023, Москва, ул.Электрозаводская, 24, +7 (495) 645-3810, a.markov@npo-echelon.ru