

**РЕШЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА УрФУ 2.3.12.13
ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ
ДОКТОРА НАУК**

от «27» декабря 2022 г. № 10

о присуждении Синадскому Николаю Игоревичу, гражданство Российской Федерации, ученой степени доктора технических наук.

Диссертация «Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите диссертационным советом УрФУ 2.3.12.13 «17» октября 2022 г., протокол № 6.

Соискатель, Синадский Николай Игоревич, 1969 года рождения;

диссертацию на соискание ученой степени кандидата технических наук защитил в 2001 г. в специальном диссертационном совете, созданном на базе Уральского государственного технического университета; в 2003 г. присвоено ученое звание доцента по специальности «Методы и системы защиты информации, информационная безопасность»;

является военнослужащим (г. Екатеринбург); по совместительству работает в должности доцента учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина».

Диссертация выполнена в учебно-научном центре «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», Минобрнауки России.

Официальные оппоненты:

Козачок Александр Васильевич – доктор технических наук, доцент, Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации», г. Орел, сотрудник Академии ФСО России;

Котенко Игорь Витальевич – доктор технических наук, профессор, Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», г. Санкт-Петербург, лаборатория проблем компьютерной безопасности, главный научный сотрудник, руководитель лаборатории;

Лось Владимир Павлович – доктор военных наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», г. Москва, Центр исследования проблем кадрового обеспечения отрасли информационной безопасности, директор

дали положительные отзывы на диссертацию.

Соискатель имеет более 50 опубликованных работ, в том числе по теме диссертации опубликовано 18 работ, из них 14 статей, опубликованных в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, включая 4 – в изданиях, входящих в международные цитатно-аналитические базы Scopus и Web of Science; 4 свидетельства о регистрации программ для ЭВМ. Общий объем опубликованных работ по теме диссертации – 10,8 п.л., авторский вклад – 4,7 п.л.

Основные публикации по теме диссертации:

Статьи в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. Gaidamakin N. File Operations Information Collecting Software Package Used in the Information Security Incidents Investigation / Gaidamakin, N., Gibilinda, R. & Sinadsky, N. // 2020 Ural Symposium on Biomedical Engineering,

Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0559-0562. (0,4 п.л./0,1 п.л.) (Scopus).

2. Gaidamakin N. Method of Forming the Static Structure of Social Graphs in the Problem of Modeling Interaction Between Users of Information and Telecommunication Services / Gaidamakin, N., **Sinadsky, N.** & Sushkov, P. // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0586-0588. (0,3 п.л./0,1 п.л.) (Scopus).

3. Semenishchev I. Method for Forming the Dynamic Components of Conditionally Real Data Arrays Based on Color Petri Net Algorithms for Organizing a Computer Training Platform for Investigating Information Security Incidents / Semenishchev, I., Sinadskiy, A., Sinadsky, M., **Sinadsky, N.** & Sushkov, P. // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2020. – pp. 0582-0585. (0,4 п.л./0,1 п.л.) (Scopus).

4. Гайдамакин Н.А. Комплексный имитационно-статистический метод синтеза массивов условно-реальных данных на основе структурно-параметрической модели взаимодействия пользователей информационно-телекоммуникационных сервисов / Гайдамакин Н.А., **Синадский Н.И.**, Сушков П.В. // Вестник УрФО. Безопасность в информационной сфере. — 2020. — № 1 (35). — С. 12–23. (1,3 п.л./0,4 п.л.)

5. Гайдамакин Н.А. Метод экспресс-анализа событий, связанных с воздействиями на файлы, предназначенный для расследования инцидентов информационной безопасности / Гайдамакин Н.А., Гибилinda Р.В., **Синадский Н.И.** // Вестник СибГУТИ. — 2020. — № 4. — С. 3-10. (0,8 п.л./0,6 п.л.)

6. Гайдамакин Н.А. Событийная модель процесса идентификации воздействий на файлы при расследовании инцидентов информационной безопасности, основанная на математическом аппарате сетей Петри / Гайдамакин Н.А., Гибилinda Р.В., **Синадский Н.И.** // Вестник СибГУТИ. — 2020. — № 1. — С. 73-88. (0,9 п.л./0,3 п.л.)

7. **Sinadskiy N.** Statistical Model for the Synthesis of Billing Information / Sinadskiy, N., Sinadskiy, A. & Semenishchev, I. // 2019 Ural Symposium on

Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT).
– 2019. – pp. 303-306. (0,4 п.л./0,1 п.л.) (Scopus, WoS)

8. Семенищев И.А. Синтез массивов биллинговой информации на основе статистико-событийной модели взаимодействия абонентов сетей сотовой связи / Семенищев И.А., Синадский А.Н., **Синадский Н.И.**, Сушков П.В. // Вестник УрФО. Безопасность в информационной сфере. — 2018. — № 1 (27). — С. 47–56. (1,0 п.л./0,4 п.л.)

9. Агафонов А.В. Автоматизация тестирования сетевых средств защиты информации на основе применения эволюционно–генетического подхода / Агафонов А.В., **Синадский Н.И.** // Математические структуры и моделирование. — 2018. — № 2 (46). — С. 125-134. (1,0 п.л./0,5 п.л.)

10. **Синадский Н.И.** Модификация методов анализа социальных графов на основе применения атрибутивных компонентов учетных записей для идентификации сообществ пользователей социальных сетей / Синадский Н.И., Сушков П.В. // Вестник УрФО. Безопасность в информационной сфере. — 2017. — № 2 (24). — С. 32–40. (0,9 п.л./0,5 п.л.)

11. Агафонов А.В. Тестирование защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании» с применением генетического алгоритма / Агафонов А.В., **Синадский Н.И.** // Вестник УрФО. Безопасность в информационной сфере. — 2017. — № 2 (24). — С. 4–8. (0,5 п.л./0,2 п.л.)

12. Агафонов А.В. Структура и принцип работы комплекса тестирования устойчивости телекоммуникационного оборудования к сетевым атакам типа «отказ в обслуживании» / Агафонов А.В., **Синадский Н.И.** // Вестник УрФО. Безопасность в информационной сфере. — 2015. — № 4 (18). — С. 4–11. (0,9 п.л./0,4 п.л.)

13. Богданов В.В. Алгоритм обнаружения комплексных компьютерных атак на основе признаков, получаемых путем формализации положений политики безопасности с использованием аппарата иерархических нечетких систем / Богданов В.В., **Синадский Н.И.** // Проблемы информационной

безопасности. Компьютерные системы. — 2008. — № 1. — С. 13–26. (1,6 п.л./0,8 п.л.)

14. Богданов В.В. Система обнаружения компьютерных атак на основе положений политики безопасности / Богданов В.В., **Синадский Н.И.** // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2007. — Т. 2. — С. 11–14. (0,4 п.л./0,2 п.л.)

Свидетельства о регистрации программ для ЭВМ

15. Свидетельство о государственной регистрации программы для ЭВМ № 2022611054. Программное обеспечение синтеза массивов данных о сетевом взаимодействии пользователей в составе учебного компьютерного полигона по расследованию инцидентов информационной безопасности / Синадский А.Н., **Синадский Н.И.** — Заявка № 2021669185 от 25.11.2021; дата государственной регистрации в Реестре программ для ЭВМ 19.01.2022.

16. Свидетельство о государственной регистрации программы для ЭВМ № 2022611053. Программное обеспечение синтеза массивов данных для стенда тестирования информационно-аналитических систем безопасности / Синадский М.Н., **Синадский Н.И.** — Заявка № 2021669809 от 27.11.2021; дата государственной регистрации в Реестре программ для ЭВМ 19.01.2022.

17. Свидетельство о государственной регистрации программы для ЭВМ № 2021681075. Программный комплекс нагрузочного тестирования систем обнаружения компьютерных атак с применением генетического алгоритма / Синадский А.Н., **Синадский Н.И.** — Заявка № 2021680589 от 05.12.2021; дата государственной регистрации в Реестре программ для ЭВМ 17.02.2022.

18. Свидетельство о государственной регистрации программы для ЭВМ № 2022611833. Программный комплекс синтеза массивов данных для стенда тестирования телекоммуникационного оборудования / Синадский А.Н., **Синадский Н.И.** — Заявка № 2021680409 от 05.12.2021; дата государственной регистрации в Реестре программ для ЭВМ 02.02.2022.

На автореферат поступили отзывы:

1. Баранковой Инны Ильиничны, доктора технических наук, доцента, заведующей кафедрой информатики и информационной безопасности ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск. Содержит замечания по аспектам моделирования сетевого трафика.
2. Богданова Валентина Викторовича, кандидата технических наук, генерального директора ООО «Уральский центр систем безопасности», г. Екатеринбург. Содержит замечания по синтезу атакующего воздействия.
3. Воронцова Юрия Витальевича, кандидата технических наук, начальника специального научно-технического отдела АО «Уральский электрохимический комбинат», г. Новоуральск. Содержит замечания по аспектам анализа соответствия сгенерированных данных реальным.
4. Гильмиярова Романа Владимировича, генерального директора ООО «Институт радиоэлектронных систем» г. Екатеринбург. Содержит замечания по критериям отбора фрагментов сетевого трафика и его объема.
5. Девянина Петра Николаевича, доктора технических наук, члена-корреспондента Академии криптографии России, профессора, научного руководителя ООО «РусБИТех-Астра», г. Москва. Содержит замечания по аспектам использования современных технологий виртуализации.
6. Дудорова Евгения Николаевича, кандидата технических наук, доцента, ведущего специалиста по информационной безопасности службы корпоративной безопасности АО «Ачимгаз», г. Новый Уренгой. Содержит замечания по вопросам проверки адекватности предложенных математических моделей.
7. Зыряновой Татьяны Юрьевны, кандидата технических наук, доцента кафедры «Информационные технологии и защита информации» ФГБОУ ВО «Уральский государственный университет путей сообщения», г. Екатеринбург. Содержит замечания по оценке степени достижения прагматической цели.

8. Королькова Юрия Дмитриевича, доктора физико-математических наук, профессора, профессора кафедры радиофизики и радиоэлектроники физического факультета ФГБОУ ВО «Иркутский государственный университет», г. Иркутск. Содержит замечания по критериям, примененным при отборе фрагментов сетевого трафика.

9. Назарова Дмитрия Михайловича, доктора экономических наук, доцента, заведующего кафедрой информационной безопасности ФГБОУ ВО «Уральский государственный экономический университет», г. Екатеринбург. Содержит замечания по интерпретации результатов проведения кибератак на сетевую инфраструктуру.

10. Нейгера Сергея Васильевича, директора по развитию бизнеса АО «Перспективный мониторинг», г. Москва. Содержит замечания по применению показателей защищенности объектов.

11. Оленникова Евгения Александровича, кандидата технических наук, доцента, доцента кафедры информационной безопасности ФГАОУ ВО «Тюменский государственный университет», г. Тюмень. Содержит замечания по недостаточности критики применяемых при тестировании ССЗИ методик и инструментов.

12. Поляковой Елены Николаевны, кандидата педагогических наук, доцента, директора Института математики и интеллектуальных систем, доцента кафедры «Безопасность информационных и автоматизированных систем» ФГБОУ ВО «Курганский государственный университет», г. Курган. Содержит замечания по выбору формы, описывающей покрытие базовых станций.

13. Пономарева Олега Павловича, доктора технических наук, доцента, заместителя генерального директора по НТР – главного конструктора АО «Уральское производственное предприятие «Вектор», г. Екатеринбург. Содержит замечания по применению статистических характеристик заголовков пакетов.

14. Соколова Александра Николаевича, кандидата технических наук, доцента, заведующего кафедрой защиты информации Высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск. Содержит замечания по возможности внесения изменений в конфигурацию ССЗИ в процессе тестирования.

15. Тимакова Алексея Анатольевича, кандидата технических наук, доцента, доцента базовой кафедры № 252 – Информационной безопасности Института кибернетики «МИРЭА – Российский технологический университет», г. Москва. Содержит замечания по применению алгоритма сдвига среднего для решения задачи кластерного анализа результатов работы генетического алгоритма.

Выбор официальных оппонентов обоснован их высокой компетентностью и известностью достижений исследований в области методов и систем защиты информации и информационной безопасности. Это подтверждается соответствующими публикациями в рецензируемых российских и международных научных изданиях.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени доктора технических наук соответствует п. 9 Положения о присуждении ученых степеней в УрФУ, является научно-квалификационной работой, в которой на основании выполненных автором исследований решена важная научная проблема создания научно-методического инструментария для проектирования и эксплуатации компьютерных полигонов на базе моделируемой интерактивной сетевой среды, внедрение которых вносит значительный вклад в развитие информационной безопасности в Российской Федерации.

Диссертация представляет собой самостоятельное законченное исследование, обладающее внутренним единством. Положения, выносимые на защиту, содержат новые научные результаты и свидетельствуют о личном вкладе автора в науку:

1. Разработанная методология создания, функционирования и эксплуатации компьютерных киберполигонов в сфере информационной безопасности обеспечивает создание программных комплексов, предназначенных для практико-ориентированной подготовки специалистов в области информационной безопасности. В основе методологии лежит комплексное использование оригинальных научно-обоснованных методов и математических моделей, в том числе: метода синтеза интерактивной сетевой среды; имитационно-статистического метода генерации синтетического трафика; метода синтеза атакующих воздействий на информационно-телекоммуникационные системы; комплекса моделей, методик и алгоритмов для тестирования устойчивости сетевых средств защиты информации.

2. Комплексный метод синтеза интерактивной сетевой среды для компьютерных полигонов, основанный на учете свойств реального трафика, циркулирующего в различных информационно-телекоммуникационных системах, обеспечивает реализацию внешних воздействий на сетевые средства защиты информации, а также оценку эффективности этих средств защиты.

3. Имитационно-статистический метод синтеза массивов условно-реального трафика, основанный на использовании пространственно-временной статистико-событийной модели взаимодействия пользователей информационно-телекоммуникационной системы, позволяет генерировать синтетический трафик, свойства которого подобны свойствам реального трафика, и на основе его использования проводить тестирование информационно-аналитических систем безопасности.

4. Метод синтеза атакующего воздействия и ситуационных задач, основанный на применении предложенной теоретико-графовой модели распространения комплексного атакующего воздействия в иерархической системе уязвимых объектов, обеспечивает формирование массивов ситуационных задач, используемых при тестировании сетевых средств защиты информации.

5. Созданный комплекс моделей, методик и алгоритмов обеспечивает автоматизированное тестирование сетевых средств защиты информации и выявление их уязвимостей к сетевым атакам, приводящим к нарушению производительности этих средств при различных сочетаниях параметров внешней среды.

Результаты исследования внедрены в учебно-научный компьютерный полигон по расследованию инцидентов ИБ, развернутый на базе учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий – РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (акт об использовании результатов от 17.02.2022); использованы при построении обучающих стендов в составе учебных центров ООО «Институт Радиоэлектронных Систем», г. Екатеринбург (акт об использовании результатов от 10.06.2022) и Екатеринбургского научно-технического центра ФГУП «НПП Гамма» (акт об использовании результатов от 09.06.2022). Разработанные методики, программное обеспечение и экспериментальные стенды были также использованы при проведении оценки защищенности образцов ТКО, применяемых в автоматизированных системах управления технологическими процессами, в ООО «Уральский центр систем безопасности», г. Екатеринбург (акты об использовании результатов от 15.12.2015, от 30.03.2020 и от 16.05.2022).

На заседании 27 декабря 2022 г. диссертационный совет УрФУ 2.3.12.13 принял решение присудить Синадскому Н.И. ученую степень доктора технических наук.

При проведении тайного голосования диссертационный совет УрФУ 2.3.12.13 в количестве 14 человек, в том числе 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 14, против – нет, недействительных бюллетеней – нет.

Председатель

диссертационного совета

УрФУ 2.3.12.13



Поршнев Сергей Владимирович

Ученый секретарь

диссертационного совета

УрФУ 2.3.12.13



Сафиуллин Николай Тахирович

27.12.2022 г.