Аналитическая справка
к программе дополнительной профессиональной подготовки (программе профессиональной переподготовки) ИТ-профиля (далее – ДПП ПП) «Криптография»

1. Целевая группа обучающихся по ДПП ПП

Программа разработана для слушателей, обучающихся по специальностям и направлениям подготовки, не отнесенным к ИТ-сфере, согласно приложению к Методике расчета показателя «Количество принятых на обучение по программам высшего образования в сфере информационных технологий за счет бюджетных ассигнований федерального бюджета (нарастающим итогом, начиная с 2021 года)», утвержденной приказом Минцифры России от 28 февраля 2022 г. № 143.

2. Трудоемкость ДПП ПП составляет 250 часов, длительность – 9 месяцев.

3. Целью ДПП ПП является формирование у слушателей, обучающихся по специальностям и направлениям подготовки, не отнесенным к ИТ-сфере, согласно приложению к Методике расчета показателя «Количество принятых на обучение по программам высшего образования в сфере информационных технологий за счет бюджетных ассигнований федерального бюджета (нарастающим итогом, начиная с 2021 года)», утвержденной приказом Минцифры России от 28 февраля 2022 г. № 143, цифровых компетенций в области создания алгоритмов и компьютерных программ, пригодных для практического применения, а также приобретение по итогам прохождения ДПП ПП новой квалификации «Специалист по защите информации в телекоммуникационных системах и сетях»

4. Приоритетная отрасль экономики, обеспечиваемая выпускниками ДПП ПП –Образование.

5. Программа ДПП ПП рассмотрена на методическом совете

Ученый совет ФИТ НГУ

6. Сведения об апробации ДПП ПП – нет

7. Наличие соглашений с организациями реального сектора экономики, обеспечивающих сотрудничество в рамках ДПП ПП

ЗАО «Центр финансовых технологий», ООО «МобайлДевелопмент», ООО «Инновационный цент «Бирюч – новые технологии».

8. ИТ-организации, с которыми образовательная организация высшего образования – участник программы стратегического академического лидерства «Приоритет-2030» (далее – вуз-участник программы) **осуществляет взаимодействие в рамках реализации ДПП ПП**

АО «Технопарк Новосибирского Академгородка»

9. Руководитель «цифровой кафедры»

Сведения о руководителе «цифровой кафедры» представлены в Приложении 1.

10. Руководитель ДПП ПП

Сведения о руководителе ДПП ПП представлены в Приложении 2.

11. Авторы и преподаватели ДПП ПП

Сведения об авторах и преподавателях ДПП ПП представлены в Приложении 3.

12. Рецензии на ДПП ПП от индустриальных партнеров, которые являются экспертами в области информационных технологий и создания алгоритмов, программ, пригодных для практического применения:

Ищукова Евгения Александровна, Южный федеральный университет (ООО «Инновационный цент «Бирюч – новые технологии») - 1 лист.

Малыгина Екатерина Сергеевна, Балтийский федеральный университет им. И.Канта (ООО «МобайлДевелопмент») – 1 лист.

Рецензии индустриальных партнеров представлены в Приложении 4.

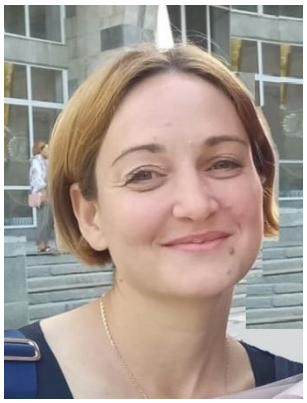
Руководитель вуза-участника
программы ректор, академик РАН М.П. Федорук

Приложение 1

ФИО руководителя «цифровой кафедры» и должность	Шашкова Марина Викторова, директор Института переподготовки и повышения квалификации/начальник управления академической политики НГУ
фотография руководителя «цифровой кафедры»	
наименование образовательной организации высшего образования – участника программы стратегического академического лидерства «Приоритет-2030»	Федеральное государственное автономное образовательное учреждение высшего образования «Новосибирский национальный исследовательский государственный университет»
информация о наличии ученой степени и/или ученого звания	кандидат экономических наук
информация о наличии стажа педагогической работы в образовательных организациях высшего образования Российской Федерации и/или стажа практической работы в профильной организации не менее 5 лет	С 2003 года по 2018 гг. – стаж педагогической деятельности в Сибирском государственном университете телекоммуникаций и информатики
информация об опыте управления проектными командами	С 2017 года участие в федеральных проектах по реализации программ ДПО ("Цифровые профессии 2021", ФП "Старшее поколение" НП "Демография", ФП "Новые возможности для каждого" НП "Образование"); Координация профилей международных и российских олимпиад (Международная олимпиада «Open Doors», Олимпиада «Я – профессионал»); организация зимних школ для студентов; С 2022 году руководство группой трансформации образовательной модели аспирантуры в НГУ.
информация об участии в научно-исследовательских проектах по направлениям, связанным с цифровыми технологиями, а также наличии публикаций по данным тематикам	Имеет опыт участия в научно-исследовательских проектах по направлениям, связанным с цифровыми технологиями, в части организации и проведения программ повышения квалификации и профессиональной переподготовки (Группа РОСНАНО, ПАО «Вымпелком» и др.)
Информация о полной занятости на «цифровой кафедре»	Полная занятость. Приказ ректора о назначении на должность руководителя цифрой кафедры.
Иная информация на усмотрение образовательной организации высшего образования – участника программы стратегического академического лидерства «Приоритет-2030»	2022 SKOLKOVO: Разработка модели будущего университета. 24 часа. 2022 SKOLKOVO: Проектно-координационная сессия ИОТконсорциума 2021 ТюмГУ: Индивидуализация в высшем образовании. Как трансформировать образовательное пространство университета. 216 час

Приложение 2

Руководитель дополнительной профессиональной подготовки (программе профессиональной переподготовки) ИТ-профиля (далее – ДПП ПП)



Наталья Николаевна Токарева (NataliaTokareva)

www.crypto.nsu.ru

Образование

2000-2004 Новосибирский государственный университет (факультет информационных технологий; бакалавриат), Новосибирск.

2004-2006 Новосибирский государственный университет (механико-математический факультет; магистратура), Новосибирск.

2006-2008 Аспирантура Института математики им. С.Л.Соболева СО РАН

2008 Защита кандидатской диссертации.

2009-н.в. старший научный сотрудник ИМ СО РАН

2011-н.в. доцент Новосибирского государственного университета

2011-н.в. руководитель Криптографического центра (Новосибирск).

2014-н.в. председатель Программного комитета Международной олимпиады по криптографии NSUCRYPTO

Области научных интересов

Криптографические булевы функции.
Криптоанализ симметричных шифров.
Блочные и поточные шифры.
Дискретная математика.

Языки

Русский (родной), английский, итальянский.

Активность

Руководитель Криптографического Центра (Новосибирск).

Научный руководитель аспирантов, магистрантов, бакалавров в области дискретной математики и криптографии. Под моим руководством защищено 5 кандидатских диссертаций, более 40 магистерских и бакалаврских работ.

Автор двух монографий и двух учебных пособий в области криптографии.

Председатель Программного комитета Международной Олимпиады по криптографии NSUCRYPTO. Руководитель и организатор Летней школы-конференции по криптографии и информационной безопасности. Руководитель научного семинара «Криптография и криптоанализ»

Член программных комитетов конференций CTCrypt, SIBECRYPT, BFA и других.

Вхожу в состав редколлегий научных журналов «Дискретный анализ и исследование операций» и «Математические труды».

Автор нескольких курсов в области криптографии: «Основы теории информации и криптографии», «Криптография и криптоанализ: современные методы» и др. в Новосибирском государственном университете.

Избранные публикации:

Монографии и учебные пособия:

- Tokareva N. Bent functions: results and applications to cryptography // Acad. Press. Elsevier, 2015. 220 pages. ISBN-10: 012802318X. ISBN-13: 978-0128023181.
- Токарева Н. Н. Симметричная криптография. Краткий курс // Учебное пособие: Новосибирский государственный университет, 2012. ISBN: 978-5-4437-0067-0. 234 с., нарусском.
- Городилова А. А., Токарева Н. Н., Шушуев Г. И. Криптография и криптоанализ. Сборник задач // Учебное пособие: Новосибирский государственный университет, 2014. ISBN: 978-5-4437-0226-1. 325 с., на русском.

Статьи:

- Tokareva N A quadratic part of a bent function can be any // Siberian Electronic Mathematical Reports, 2022. pp. 342-347. DOI 10.33048/semi.2022.19.029.
- Agievich S., Gorodilova A., Idrisova V., Kolomeec N., Shushuev G., Tokareva N. Mathematical problems of the second international students' Olympiad in cryptography // Cryptologia. V. 41. No 6. P. 534-565. 2017. DOI: 10.1080/01611194.2016.1260666
- Tokareva N., Gorodilova A., Agievich S., Idrisova V., Kolomeec N., Kutsenko A., Oblaukhov A., Shushuev G. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography // Прикладнаядискретнаяматематика. 2018. No 40. С. 34–58. DOI: 10.17223/20710410/40/4

- Gorodilova A., Agievich S., Carlet C., Gorkunov E., Idrisova V., Kolomeec N., Kutsenko A., Nikova S., Oblaukhov A., Picek S., Preneel B., Rijmen V., and Tokareva N. Problems and solutions from the fourth International Students' Olympiad in Cryptography (NSUCRYPTO) // Cryptologia. 2019, Vol. 43, No. 2, pp. 138–174. DOI: 10.1080/01611194.2018.1517834
- Gorodilova A., Agievich S., Carlet C., Hou X., Idrisova V., Kolomeec N., Kutsenko A., Mariot L., Oblaukhov A., Picek S., Preneel B., Rosie R., Tokareva N. The Fifth International Students' Olympiad in Cryptography - NSUCRYPTO: problems and their solutions // Cryptologia 2020, Vol. 44, I. 3, pp. 223-256. (Published online 21 October 2019) 2020. DOI: 10.1080/01611194.2019.1670282.
- A. Gorodilova, N. N. Tokareva, S. V. Agievich, C. Carlet, E. V. Gorkunov, V. A. Idrisova, N. A. Kolomeec, A. V. Kutsenko, R. K. Lebedev, S. Nikova, A. K. Oblaukhov, I. A. Pankratova, M. A. Pudovkina, V. Rijmen, A. N. Udovenko. On the Sixth International Olympiad in Cryptography NSUCRYPTO // Journal of Applied and Industrial Mathematics volume 14, 623–647(2020). DOI: https://doi.org/10.1134/S1990478920040031
- Tokareva N.N., Shaporenko A.S., Solé P. Connections between quaternary and Boolean bent functions, Siberian Electronic Mathematical Reports, 2021. pp. 561-578. DOI 10.33048/semi.2021.18.041 http://semr.math.nsc.ru/v18/n1/p561-578.pdf
- Gorodilova A. A., Tokareva N. N., Agievich S. V., Carlet C., Idrisova V. A., Kalgin K. V., Kolegov D. N., Kutsenko A. V., Mouha N., Pudovkina M. A., Udovenko A. N. The Seventh International Olympiad in Cryptography: problems and solutions, SEMR, Volume 18 (2021), N 2, pp. A4-A29. DOI 10.33048/semi.2021.18.063
- Mouha N., Kolomeec N., Akhtyamov D., Sutormin I., Panferov M., Titova K., Bonich T., Ischukova E., Tokareva N., Zhantulikov B. Maximums of the Additive Differential Probability of Exclusive-Or // IACR Transactions on Symmetric Cryptology, Volume 2021, Issue 2, 2021. Pages 292-313. DOI: https://doi.org/10.46586/tosc.v2021.i2.292-313.
- B. Bilgin, S. Nikova, V. Nikov, V. Rijmen, N. Tokareva, V. Vitkup Threshold implementations of small S-boxes // Cryptography and Communications. 2015. V. 7. N 1. P. 3-33.
- Tokareva N.N. On decomposition of a Boolean function into sum of bent functions // Siberian Electronic Math. Reports. 2014. V. 11. P. 745-751.
- Tokareva N. Duality between bent functions and affine functions // Discrete Mathematics, V. 312. 2012. P. 666-670.
- Tokareva N. On the number of bent functions from iterative constructions: lower bounds and hypotheses // Advances in Mathematics of Communications (AMC). 2011. V. 5, N 4. P. 609-621.
- Tokareva N. N. The group of automorphisms of the set of bent functions // Discrete Mathematics and Applications. 2010. V. 20. N 5-6. P. 655-664.
- Tokareva N. N. Generalizations of bent functions. A survey // Discrete Analysis and Operation Research. 2010. V. 17. N 1. P. 34-64 in Russian. English translation: Journal of Applied and Industrial Mathematics, 2011, V. 5. N 1. P. 110-129.

Приложение 3

В число преподавателей программы входят не менее 30 специалистов:

• GANGOPADHYA Sugata – PhD, декан факультета электроники и техники связи Индийского технологического института Рурки (г.Рурки, Индия);
• АЛЕКСЕЕВ Евгений Константинович – к.ф.-м.н., начальник отдела криптографических исследований, КРИПТО-ПРО (г.Москва);
• АТУТОВА Наталья Дмитриевна – студентка ММФ НГУ;
• БАХАРЕВ Александр Олегович – преподаватель НГУ, студент ММФ НГУ;
• БОНИЧ Татьяна Андреевна – преподаватель СУНЦ НГУ, аспирантка ФИТ НГУ;
• БЫКОВ Денис Александрович – преподаватель НГУ, студент ММФ НГУ;
• ГОРОДИЛОВА Анастасия Александровна – к.ф.-м.н., старший преподаватель кафедры теоретической кибернетики ММФ НГУ, н.с. ИМ СО РАН;
• ДОРОНИН Артемий Евгеньевич – преподаватель НГУ, аспирант ФИТ НГУ;
• ЗЮБИНА Дарья Александровна – преподаватель СУНЦ НГУ, магистрантка ФИТ НГУ;
• ИДРИСОВА Валерия Александровна – к.ф.-м.н., н.с. Института математики им. С.Л.Соболева СО РАН;
• ИЩУКОВА Евгения Александровна – к.т.н., доцент кафедры безопасности информационных технологий Южного федерального университета (г.Ростов-на-Дону);
• КАЛГИН Константин Викторович – к.ф.-м.н., старший преподаватель кафедры параллельного программирования ФИТ НГУ, м.н.с. ИВМиМГ, н.с. ИМ СО РАН;
• КОЛЕГОВ Денис Николаевич – к.т.н., доцент кафедры компьютерной безопасности ТГУ, главный разработчик облачной платформы кибербезопасности компании Bi.Zone (Томск);
• КОЛОМЕЕЦ Николай Александрович – к.ф.-м.н., старший преподаватель кафедры теоретической кибернетики ММФ НГУ;
• КОНДЫРЕВ Дмитрий Олегович – аспирант ФИТ НГУ, ассистент кафедры компьютерных систем ФИТ НГУ;
• КОСТОЧКА Светлана Владимировна – преподаватель кафедры физвоспитания НГУ;

• КУЦЕНКО Александр Владимирович – к.ф.-м.н., ассистент кафедры теоретической кибернетики ММФ НГУ;
• КЯЖИН Сергей Николаевич – к.ф.-м.н., ведущий инженер-аналитик отдела криптографических исследований, КРИПТО-ПРО (г.Москва);
• МАКСИМЛЮК Юлия Павловна – аспирантка ММФ НГУ, ассистент кафедры компьютерных систем ФИТ НГУ;
• МАЛЫГИНА Екатерина Сергеевна – к.ф.-м.н., доцент Балтийского федерального университета им. И. Канта (г.Калининград);
• МЕЛЬНИЧУК Евгений Михайлович – главный расследователь BLIN.agency, ассистент Балтийского федерального университета им. И. Канта (г.Калининград);
• МОКРОУСОВ Антон Сергеевич – магистрант ФИТ НГУ;
• НИКОЛАЕВ Антон Анатольевич – разработчик сервисов анализа защищенности Bi.Zone, главный разработчик фрэймворка Grinder (Томск);
• ПАНКРАТОВА Ирина Анатольевна – доцент Томского государственного университета, к.ф.-м.н.
• ПАНФЕРОВ Матвей Андреевич – преподаватель СУНЦ НГУ, аспирант ИМ СО РАН;
• ПАРФЕНОВ Денис Романович – преподаватель НГУ, магистрант ФИТ НГУ;
• СУТОРМИН Иван Александрович – магистрант ММФ НГУ;
• ТОКАРЕВА Наталья Николаевна – к.ф.-м.н., доцент кафедры компьютерных систем ФИТ, кафедры теоретической кибернетики ММФ, с.н.с. ИМ СО РАН;
• ХИЛЬЧУК Ирина Сергеевна – преподаватель НГУ, магистрантка ММФ НГУ;
• ШАПОРЕНКО Александр Сергеевич – аспирант ММФ НГУ, ассистент кафедры дискретного анализа и исследования операций ФИТ НГУ.

100% общего объема аудиторных или приравненных к ним часов в рамках ДПП ПП реализуются научно-педагогическими работниками отвечающим следующим требованиям:

- наличие высшего профильного образования в ИТ-отрасли и/или дополнительного профессионального образования – профессиональной переподготовки в части, касающейся профессиональных компетенций в области создания алгоритмов и программ, пригодных для практического применения;

- наличие стажа педагогической работы в образовательных организациях высшего образования Российской Федерации и/или стажа практической работы в профильной организации ИТ-отрасли не менее 3 лет.

РЕЦЕНЗИЯ

на дополнительную профессиональную программу профессиональной переподготовки "Криптография"

В последние годы скорость развития и изменения киберпространства растет экспоненциально на фоне развития объема обрабатываемых данных, числа подключенных к интернету устройств и сервисов, а также самих технологий. Этот тренд особенно набирает обороты в связи со всеобщей цифровизацией и перехода работы многих компаний на частичный онлайн режим. Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Дополнительная профессиональная программа «Криптография», разработанная в ФГ АОУ ВО «Новосибирский национальный исследовательский государственный университет», представляет собой актуальный курс для обучения широкого круга лиц, имеющих образование в области ИТ, математики или физики.

Программа состоит из пяти модулей, в которых подробно разобраны принципы работы блокчейн-технологии, методов обработки и защиты информации, представлены основы криптографического анализа. Изложение теоретического материала сопровождается описанием математических методов криптографии на доступном для понимания языке, также представлен тематика, затрагивающая постквантовое криптографическое направление. Кроме того, объясняются основы языков программирования C++ и Python, необходимые для криптографических приложений, что способствует высокой степени вовлеченности слушателей курса в практическую работу по применению полученных знаний в области криптографии и информационной безопасности.

Курс является практико-ориентированным, поскольку включает в себя как исследовательский модуль, так и практику – участие в международной криптографической олимпиаде. Прохождение представленной программы позволит слушателям освоить новые компетенции цифровой экономики и представит возможность найти свое место на рынке труда.

Доцент, научный сотрудник
лаборатории «Математические методы
защиты и обработки информации»
Балтийского федерального университета им. И.Канта,
к.ф.-м.н. Малыгина Е.С.

РЕЦЕНЗИЯ

на программу ДПО

«Криптография »

Программа профессиональной переподготовки «Криптография и информационная безопасность: Международные исследования и прикладные разработки» осуществляется на базе Криптографического центра г. Новосибирска. Основной целью данной программы является развитие исследовательского потенциала и подготовка современных специалистов в области криптографии и информационной безопасности. Можно с уверенностью сказать, что данная программа профессиональной переподготовки не имеет аналогов в РФ.

Программа состоит из пяти блоков, каждый из которых дает глубокий и разносторонний охват различных областей криптографии. Слушателям предлагается курс лекций от ведущих специалистов в области криптографии, в том числе зарубежных. Знания, полученные в ходе прослушивания лекций, закрепляются на практике в ходе выполнения научного исследования на заданную тему. Слушатели работают командами, что дополнительно обеспечивает обмен опытом и развитие практических навыков. Также в одном из блоков программы предусмотрено решение задач международной олимпиады NSUCRYPTO, задачи для которой составляются ведущими учеными в области математики и криптографии.

Таким образом, слушатели в результате прохождения программы получают уникальную подборку знаний в области современной криптографии от российских и зарубежных специалистов в данной области, а также получают бесценный практический опыт проведения исследований в данной области – от постановки современной проблемы, командной работы по ее решению под руководством опытных исследователей до получения результата и его публикации.

Считаю, что программа ДПО «Криптография и информационная безопасность: Международные исследования и прикладные разработки» является уникальной и обязательно должна быть реализована на территории РФ.

к.т.н., доцент,
доцент каф. БИТ ИКТИБ ЮФУ Ищукова Е.А.