

Статья посвящается памяти Владимира Владимировича Сухомлина, помогавшему автору в создании нового образовательного направления на начальном этапе работы

УДК 378.016:004
DOI: 10.25559/SITITO.17.202103.724-734

Научная статья

Создание профиля «Кибербезопасность и искусственный интеллект» для направления подготовки ФИИТ на основе куррикулумного подхода

В. А. Сухомлин

ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова», г. Москва, Российская Федерация
119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1
sukhomlin@mail.ru

Аннотация

Статья посвящена описанию основных характеристик профиля «Кибербезопасность и искусственный интеллект» для направления подготовки 02.03.02 Фундаментальная информатика и информационные технологии (ФИИТ). Рассмотрены концепция и история создания базового направления ФИИТ, его назначение как многопрофильного стандарта, предназначенного для подготовки высококвалифицированных ИТ-специалистов по широкому спектру ИТ-направлений. Отмечается, что ФИИТ отвечает современным тенденциям развития области ИТ и ИТ-образования, в частности, духу документов Computing Curricula 2005 и Computing Curricula 2020. Рассмотрены основные принципы разработки и архитектура свода знаний куррикулума дисциплины «Кибербезопасность», на основе которого разработан профиль «Кибербезопасность и искусственный интеллект». Приведено описание общих характеристик данного профиля, включая: цели, миссию, профессиональные компетенции как ожидаемые результаты обучения. Архитектурный подход к проектированию свода знаний куррикулума кибербезопасности позволил системным образом выявить набор знаниевых доменов, определяющих содержание программ подготовки бакалавров кибербезопасности.

Ключевые слова: ИТ-образование, цифровые навыки, компетенции, профили ИТ-образования, стандарты цифровых навыков и компетенций, фреймворки для описания ролей/навыков/компетенций в области ИТ, система навыков для информационного века SFIA, куррикулум, компьютеринг, результаты обучения, своды знаний, своды профессиональных знаний, промышленные своды знаний, стандарты куррикулумов, кибербезопасность, информационная безопасность, архитектурная модель кибербезопасности, искусственный интеллект

Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Сухомлин, В. А. Создание профиля «Кибербезопасность и искусственный интеллект» для направления подготовки ФИИТ на основе куррикулумного подхода / В. А. Сухомлин. – DOI 10.25559/SITITO.17.202103.724-734 // Современные информационные технологии и ИТ-образование. – 2021. – Т. 17, № 3. – С. 724-734.

© Сухомлин В. А., 2021



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.



The article is dedicated to the memory of Vladimir Vladimirovich Sukhomlin, who assisted the author at the initial stage of developing a new field of education

Original article

Creating a Profile "Cybersecurity and Artificial Intelligence" for the Direction of FIIT Training Based on the Curriculum Approach

V. A. Sukhomlin

Lomonosov Moscow State University, Moscow, Russian Federation

1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation

sukhomlin@mail.ru

Abstract

The article describes the main characteristics of the profile "Cybersecurity and artificial intelligence" for the direction of training 02.03.02 Fundamental Informatics and Information Technology (FIIT). The concept and history of the creation of the basic direction of FIIT, its purpose as a multidisciplinary standard designed to train highly qualified IT professionals in a wide range of IT areas are considered. It is noted that FIIT meets modern trends in the development of IT and IT education, in particular, the spirit of the documents ComputingCurricula 2005 and ComputingCurricula 2020. The main principles of development and architecture of the code of knowledge of the curriculum of the discipline "Cybersecurity" are considered, on the basis of which the profile "Cybersecurity and Artificial Intelligence" is developed. A description of the general characteristics of this profile is given, including: goals, mission, professional competencies as expected learning outcomes.

Keywords: IT education, digital skills, competencies, IT education profiles, digital skills and competencies standards, IT role/skill/competency frameworks, SFIA skills framework for the information age, curriculum, computing, learning outcomes, body of knowledge (BoK), codes of professional knowledge, industrial codes of knowledge, curriculum standards, cybersecurity, information security, architectural model of cybersecurity, artificial intelligence

The author declares no conflict of interest.

For citation: Sukhomlin V.A. Creating a Profile "Cybersecurity and Artificial Intelligence" for the Direction of FIIT Training Based on the Curriculum Approach. *Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education*. 2021; 17(3):724-734. DOI: <https://doi.org/10.25559/SITITO.17.202103.724-734>



История и концепция создания направления подготовки «Фундаментальная информатика и информационные технологии»

История направления подготовки «Фундаментальная информатика и информационные технологии» (ФИИТ) начинается с 2002 г., когда по инициативе автора статьи и на основе разработанных им концепции и проектов государственных стандартов Приказом Министерства образования РФ № 4175 от 29.11.2002 было создано новое направление подготовки бакалавров и магистров 511900 «Информационные технологии»¹. Основная идея создания этого направления состояла в том, чтобы сформировать магистральное многопрофильное направление подготовки профессиональных кадров в области информационных технологий (ИТ) на основе классического университетского образования. В связи с чем новое направление 511900 «Информационные технологии» создавалось как аналог направления Computing (по существу академическое название области информационных технологий), но на более фундаментальной математической и алгоритмической базе, характерной для классического университетского образования. Предполагалось, что новое направление станет магистральным для национальной системы ИТ-образования, адекватно отражающим специфику, тенденции, динамику развития научных и прикладных аспектов области ИТ, и способным объединить в целостную систему ИТ-образования все другие образовательные деятельности, связанные с ИТ, включая смежные специальности и направления, дать им основу и важные ориентиры для развития.

В постановочной части Приказа № 4175 говорилось: «В соответствии с решением Межведомственного экспертного совета по государственному образовательному стандарту высшего профессионального образования от 04.07.2002, а также учитывая потребность в соответствующих кадрах, приказываю:

1. Создать в экспериментальном порядке направление подготовки бакалавров и магистров 511900 Информационные технологии со степенью (квалификацией) «бакалавр информационных технологий» и «магистр информационных технологий».
2. Отнести направление «Информационные технологии» к группе 510000 «Естественные науки и математика».
3. Ввести в экспериментальном порядке, начиная с 2003/2004 учебного года, подготовку по направлению «Информационные технологии» в Московском государственном университете имени М. В. Ломоносова; Санкт-Петербургском государственном университете; Нижегородском государственном университете им. Н. И. Лобачевского; Московском государственном институте электроники и математики (техническом университете); Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» им. В.И. Ульянова (Ленина); «МАТИ» – Российском государственном технологическом университете им. К.Э. Циолковского...»².

Данный приказ явился значимой вехой в системе высшего образования, а именно, он ознаменовал признание области ИТ как самостоятельного научного и прикладного направления и самостоятельной университетской дисциплины, которая заняла свое место в системе классического университетского образования наряду с математикой, физикой, химией, биологией. Также он дал старт эксперименту по внедрению данного направления в систему высшего образования страны.

Эксперимент по внедрению данного направления, начавшийся в 2003 г., проходил весьма успешно и показал большую заинтересованность вузов в данном направлении. Поэтому на совещании «Актуальные проблемы информатики в современном российском образовании», которое проводил 26 февраля 2005 г. в МГУ имени М. В. Ломоносова НМС по информатике (Научно-методический совет по информатике при Министерстве образования и науки РФ), было принято решение о переводе его из экспериментальной фазы в фазу практического внедрения. В решении говорилось следующее: «1. Одобрить инициативу факультета ВМК МГУ имени М. В. Ломоносова по созданию образовательного направления «Информационные технологии», имеющего большое научное и практическое значение, а также проделанную факультетом работу по формированию нормативно-методической базы для реализации данного направления на практике. 2. Считать целесообразным, начиная с 2005/2006 учебного года, перевод эксперимента по освоению образовательного направления «Информационные технологии» в фазу практического внедрения, обеспечив к 2008 г. охват в подготовке выпускников по данному направлению не менее 30% классических и технических университетов страны. Также рассмотреть возможность реализации данного направления вузами другого профиля (педагогическими, техническими, экономическими). В связи с чем, выйти с соответствующим предложением в Министерство образования и науки».

Неоценимый вклад в создание и становление нового направления, его доведения до высокого университетского уровня внесли: декан факультета ВМК МГУ академик Е. И. Моисеев, декан факультета ПМ-ПУ СПбГУ профессор Л. А. Петросян, профессор Е. И. Веремей и С. Н. Андрианов, доцент В. В. Евстафьева (ПМ-ПУ СПбГУ), профессор, декан Я. М. Ерусалимский (тогда РГУ), декан ННГУ имени Лобачевского В. П. Савельев, профессор В. П. Гергель, доцент О. А. Кузенков (ННГУ), декан Э. И. Коломиец и профессор А. Н. Коварцев (тогда СГАУ), декан профессор Р. Х. Латыпов (КГУ), декан, профессор А. Н. Шашкин (ВГУ), декан, профессор А. В. Язенин (ТвГУ), заместитель декана факультета ВМК МГУ по методической работе доцент В. В. Тихомиров.

После перевода данного направления в фазу внедрения список реализующих его вузов стал быстро расти. В этот период, в 2006 г., по предложению автора направление «Информационные технологии» было переименовано в направление «Фундаментальная информатика и информационные технологии», что в большей мере отражало заложенную в него первоначально ориентации на фундаментальность подготовки,

¹ ГОС ВПО – бакалавриат и магистратура по направлению подготовки 511900 Информационные технологии: утв. приказом Министерства образования Российской Федерации 29 ноября 2002 г. № 4175.

² Там же.



свойственную классическим университетам. Таким образом направление ФИИТ стало непосредственным преемником направления 511900 «Информационные технологии», унаследовав от него базовые принципы. Поэтому днем создания ФИИТ следует считать дату издания Приказа Министерства образования РФ № 4175, т.е. 29.11.2002 г.

Как отмечалось, ФИИТ унаследовал базовые принципы своего предшественника³, основными из которых являлись:

- ориентация на подготовку высокопрофессиональных ИТ-специалистов, востребованных в индустрии, бизнесе и исследовательских центрах, способных развивать научно-методические основы ИТ, разрабатывать стандарты, спецификации и профили ИТ, создавать системы, продукты и сервисы новых ИТ;
- соответствие базовой профессиональной подготовки (бакалавриата) международным рекомендациям к объему знаний курикула для компьютерных наук;
- сохранение традиций российского университетского образования в углубленной, целенаправленной математической подготовке, составляющей основу фундаментальности профессионального ИТ-образования;
- обеспечение возможности интеграции российского образования в области ИТ в международную образовательную систему и выхода на международный рынок образовательных услуг и др.

Изначально в стандарт направления 511900 «Информационные технологии», а затем и в ФИИТ были заложены два равноценных базовых образовательных ядра – математическое и компьютерные науки. Последнее разрабатывалось на основе актуального международного стандарта для компьютерных наук (Computer Science Curriculum). Стандарт бакалавра вновь созданного направления был разработан таким образом, что суммарный объем учебной нагрузки для двух ядерных компонентов учебной программы составлял не более половины общей нагрузки для бакалаврских программ. Оставшуюся часть учебных часов предполагалось, в частности, использовать для профилированной подготовки по актуальным направлениям компьютеринга (т.е. области ИТ) [1]. Такой подход оставлял возможность быстрой реакции на вызовы стремительно развивающейся области ИТ путем создания новых профилей подготовки, соответствующих актуальным технологическим направлениям. При этом для каждого профиля сохранялся высокий уровень математической и алгоритмической подготовки, что позволяло готовить не просто профессиональные кадры конкретной специализации, а выпускать потенциальных исследователей и разработчиков новых ИТ профильных направлений [2-4].

Подход, заложенный в ФИИТ, хорошо коррелируется с современными тенденциями, изложенными в Computing Curricula 2005 (CC2005)⁴ и Computing Curricula 2020 (CC2020)⁵. В частности, в CC2020 компьютеринг определяется как метадисциплина, объединяющая непрерывно расширяющееся множество технологических направлений области ИТ.

Однако потенциал направления ФИИТ как расширяемой платформы для разработки профилей подготовки профессиональных кадров по актуальным направлениям ИТ использовался до настоящего времени не в полной мере.

Первым таким профилем по существу стала образовательная программа «Программирование и информационные технологии», разработанная и внедренная в практику в 2003 в СПбГУ на факультете ПМ-ПУ профессором Е. И. Веремеем. Данная программа была ориентирована на подготовку разработчиков моделей и программного обеспечения систем управления⁶.

Следующим профилем для направления ФИИТ стала образовательная программа «Программная инженерия», разработанная профессором А. Н. Тереховым в 2006 г., которая использовалась в течение нескольких лет в СПбГУ для подготовки бакалавров по программной инженерии. В частности, в статье [5] отмечалось «Мы считаем, что наилучшим кандидатом на роль базового стандарта образования в области информатики и программной инженерии является направление подготовки бакалавров и магистров 511900 "Информационные технологии" [автор В. А. Сухомлин].»

Позитивные тенденции в профилировании ФИИТ наметились, начиная с 2021 г. а именно, с 2021 г. в СПбГУ стартовало обучение по профилю ФИИТ «Большие данные и распределенная цифровая платформа», разработанного профессором А. Б. Дегтяревым на факультете ПМ-ПУ СПбГУ⁷. Также в 2021 г. автором статьи разработан профиль «Кибербезопасность и искусственный интеллект», который и описан ниже. Рассматриваемый профиль разработан на основе модели цифровых навыков кибербезопасности (МНК) [6] и свода знаний кибербезопасности (СЗК) [7] – результатов исследовательского проекта, выполненного автором с научно-исследовательской группой на кафедре информационной безопасности факультета ВМК МГУ. Рассмотрим кратко архитектуру МНК и соответствующего ему СЗК.

Архитектура свода знаний кибербезопасности

Основным содержанием курикула кибербезопасности является описание СЗК, разработанного на основе МНК в соответствии с концепцией цифровых навыков [8-10]. Домен-

³ В. А. Сухомлин, В. В. Сухомлин. Концепция нового образовательного направления [Электронный ресурс] // Открытые системы. СУБД. 2003. № 2. URL: <https://www.osp.ru/os/2003/02/182628> (дата обращения: 24.07.2021).

⁴ Computing Curricula 2005 (CC2005) / ed. by CORPORATE The Joint Task Force on Computing Curricula. ACM, IEEE Press, 2006. 56 p.

⁵ Computing Curricula 2020: Paradigms for Global Computing Education / ed. by CC2020 Task Force. ACM, New York, NY, USA, 2020. 205 p. doi: <https://doi.org/10.1145/3467967>

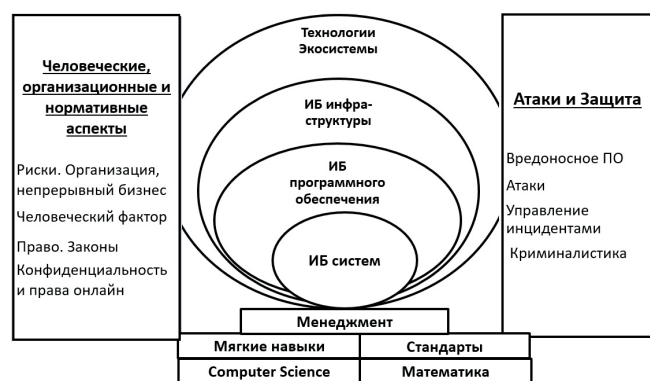
⁶ Образовательная программа «Программирование и информационные технологии» по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» Факультета прикладной математики – процессов управления СПбГУ [Электронный ресурс]. URL: <https://spbu.ru/postupayushchim/programms/bakalavriat/programmirovaniye-i-informacionnyye-tehnologii> (дата обращения: 24.07.2021).

⁷ «Большие данные и распределенная цифровая платформа» профиль бакалавриата 02.03.02 «Фундаментальная информатика и информационные технологии» Факультета прикладной математики – процессов управления СПбГУ [Электронный ресурс]. URL: <https://spbu.ru/postupayushchim/programms/bakalavriat/bolshie-dannye-i-raspredelelnaya-cifrovaya-platforma> (дата обращения: 24.07.2021).



но-ориентированная архитектура МЦН представляет собой многоуровневую иерархическую структуру. На верхнем уровне этой структуры располагаются **категории доменов навыков** (КДН), объединяющие навыки одного или нескольких доменов, каждый из которых в свою очередь структурируется на **модули** навыков, состоящие из одного или нескольких предметных навыков, определяющих требования к знаниям и умениям в некоторой предметной области, приобретение которых требуется для формирования профессиональных навыков кибербезопасности. Далее в тексте вместо понятий предметные и профессиональные навыки будет использоваться просто навыки.

Архитектура МНК высокого уровня (на уровне категорий доменов навыков) иллюстрируется на рисунке 1.



Р и с. 1. Модель навыков кибербезопасности высокого уровня (на уровне категорий доменов навыков) [6; С. 704]

F i g. 1. High Level Cybersecurity Skills Model (at skill domain category level) [6; p. 704]

МНК включает в свой состав следующие категории навыков:

1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)
2. Атаки и Защита (Attacks and Defences)
3. Безопасность систем (System Security)
4. Безопасность программного обеспечения и платформ (Software and Platform Security)
5. Безопасность инфраструктуры (Infrastructure Security)
6. Безопасность технологий (Technology Security)
7. Базовые навыки компьютерных наук (Computer Science)
8. Математика для кибербезопасности (Cybersecurity math)
9. Менеджмент проектов и системы менеджмента качества (Project management and quality management systems)
10. Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills)
11. Секторальные навыки (Sector skills).

Как отмечалось, центральной частью куррикулума кибербезопасности является описание свода знаний (СЗК), необходимых для развития навыков, определенных в МНК. Так как в концепции навыков ключевым элементом навыка служит объем знаний, необходимый для успешной реализации функциональности навыка, архитектура СЗК представляет собой структуру аналогичную архитектуре МНК, с тем отличием, что элементы этой структуры интерпретируются не как совокупности навыков, а как совокупности знаний и умений им соответствующих [11-17].

Архитектурный подход к проектированию СЗК куррикулума кибербезопасности позволил системным образом выявить набор знаниевых доменов, определяющих содержание программ подготовки бакалавров кибербезопасности.

В частности, домены знаний, непосредственно связанные с проблематикой кибербезопасности составили набор, представленный в Таблице 1.

Т а б л и ц а 1. Набор доменов знаний, непосредственно связанных с кибербезопасностью
T a b l e 1. A set of knowledge domains directly related to cybersecurity

Категории	Домены знаний
1. Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)	1. Управление рисками и непрерывностью бизнеса – УР (Risk and Business Continuity Management – RM) 2. Юридические и нормативные аспекты ИБ – ЮНА (Legal and regulatory aspects of information security – LRA) 3. Человеческие факторы в ИБ – ЧФ (Human Factors in Information Security – HF) 4. ИБ онлайн-деятельности – БОД (Information Security of Online Activities – SOA)
2. Атаки и Защита (Attacks and Defences)	5. Вредоносные программы и средства защиты – ВП (Malware and means of protection – MMP) 6. Роли и модели атак – РМА (Roles and Models of Cyber Attacks –RMA) 7. Операции и управление инцидентами ИБ – ОУИ (Information Security Operations and Incident Management – OIM) 8. Цифровая криминалистика – ЦК (Digital Forensics – DF)
3. Безопасность систем	9. Криптография – КР (Cryptography – CR) 10. Безопасность операционных систем и виртуализации – БОСВ (Operating System and Virtualization Security – OSVS) 11. Безопасность распределенных систем – БРС (Security of Distributed Systems – SDS) 12. Аутентификация, авторизация и учетность – ААН (Authentication, Authorization, and Reporting – AAR)
4. Безопасность программного обеспечения и платформ (Software and Platform Security)	13. Безопасность программного обеспечения – БПО (Software security – SWS) 14. Безопасность веб-платформ и веб-сервисов – БВВ (Security of web platforms and web services – SWW)



Категории	Домены знаний
5. Безопасность инфраструктуры (Infrastructure Security)	15. Сетевая безопасность (Network Security) 16. Безопасность аппаратного уровня (Hardware Security) 17. Безопасность кибер-физических систем (Cyber-Physical Systems Security) 18. Безопасность физического уровня и телекоммуникаций (Physical Layer & Telecommunications Security)
6. Безопасность технологий	19. Безопасность технологий Больших Данных – ББД (Security of Big Data technologies – SBD) 20. Безопасность Интернета вещей – БИВ (IoT security – IOTS)

Всего в СЗК входит более 50 доменов знаний, которые структурируются на модули знаний, темы и подтемы. Состав доменов, относящихся к ядру компьютерных наук, соответствует требованиям актуализированной версии международного стандарта куррикула по компьютерным наукам (Computer Science – CS2013)⁸. Для целей настоящей статьи нас будет интересовать домен «Интеллектуальные системы».

Домен «Интеллектуальные системы» предназначен для развития знаний и умений, способствующих решению задач с использованием методов и технологий искусственного интеллекта. Решения задач, которые относятся к сфере искусственного интеллекта, основывается на широком наборе общих и специализированных схем представления знаний, механизмах решения проблем и методах машинного обучения. Они имеют дело с восприятием (например, распознавание образов и речи, понимание естественного языка, компьютерное зрение), решением задач поиска и планирования, методами управления автономными автоматическими устройствами (роботами, дронами, самоходными автомобилями), задачами создания высокоавтоматизированных систем (агенты, мульти-агенты) [18-23].

Данный домен содержит следующие модули:

ИС / Концептуальные основы искусственного интеллекта (ИИ)
ИС / Эвристическое программирование, игры, методы решения сложных задач

ИС / Доказательство теорем в исчислении предикатов

ИС / Модели представления знаний

ИС / Машинное обучение и интеллектуальный анализ больших данных

ИС / Агенты и мультиагентные системы

ИС / Искусственные нейронные сети (ИНС) и машинное обучение ИНС

ИС / Основы технического зрения

ИС / Робототехника

Указанные выше модули знаний домена «Интеллектуальные системы», дополненные при необходимости специальными курсами углубленного изучения отдельных вопросов ИИ, представляют собой основу для формирования учебной программы профиля «Кибербезопасность и искусственный интеллект», с помощью которой могут быть подготовлены кадры с профессиональными компетенциями, определенными в разделе 3.

Рассмотрим характеристики профиля «Кибербезопасность и искусственный интеллект»⁹, включая планируемые результа-

ты освоения образовательной программы профиля, сформулированные в виде профессиональных компетенций.

Характеристики профиля «Кибербезопасность и искусственный интеллект» для направления 02.03.02 Фундаментальная информатика и информационные технологии

К основным характеристикам профиля, рассмотренным в данной статье относятся: назначение профиля, цели, планируемые результаты освоения образовательной программы (в частности, профессиональные компетенции). Рассмотрим эти характеристики подробнее.

Назначение

Основная образовательная программа бакалавриата «Кибербезопасность и искусственный интеллект» предназначена для подготовки высокопрофессиональных кадров в области информационной безопасности, способных:

- решать задачи обеспечения безопасности функционирования технологических платформ, систем и сервисов ИТ, а также процессов автоматизации социально-производственной деятельности;
- создавать доверенные технологические платформы, системы и сервисы ИТ;
- разрабатывать методы и инструментальные средства для повышения безопасности функционирования технологических платформ, систем и сервисов ИТ, в том числе с применением методов искусственного интеллекта (ИИ), анализа больших данных и других современных технологий;
- формулировать математические постановки задач в области безопасности систем искусственного интеллекта, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения, разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения;
- выполнять исследования и разработки инновационных решений в области кибербезопасности для новых информационных технологий, включая: суперкомпьютерные вычисления, Интернет вещей, промышленный интер-

⁸ Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (CS2013) / ed. by CORPORATE The Joint Task Force on Computing Curricula. ACM, New York, NY, USA, 2013. 518 p. doi: <https://doi.org/10.1145/2534860>

⁹ Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017) / ed. by Joint Task Force on Cybersecurity Education. ACM, IEEE, AIS, IFIP, New York, NY, USA, 2017. 123 p. doi: <https://doi.org/10.1145/3184594>



- нет, мобильные сетевые технологии новых поколений, грид-технологии, облачные и граничные вычисления, туманные вычисления, информационные системы систем, Большие данные и аналитику Больших данных, системы с интенсивным использованием данных, технологии распределенного реестра, технологии искусственного интеллекта, кибер-физические системы, умные города, умные производства, ВМ-технологии и технологии цифровых двойников, геоинформационные технологии, технологии виртуальной и дополненной реальности (иммерсивные технологии), технологии цифрового транспорта, робототехнические системы, инжиниринг предприятий цифровой экономики, цифровые социально-ориентированные технологии, а также различные наукоемкие приложения;
- адаптироваться к новым технологиям и осваивать новые навыки и методы работы в разнообразных контекстах, благодаря фундаментальной математической и прикладной подготовке, глубоким знаниям основ компьютерных наук.

Цели

Реализация и широкое внедрение в практику образовательной программы «**Кибербезопасность и искусственный интеллект**», разработанной на основе системного (сочетающего ориентацию на знания и компетенции/навыки) подхода с целью подготовки высокопрофессиональных кадров (бакалавров), способных решать сложные практические задачи кибербезопасности, выполнять исследования и анализ проблем информационной безопасности, связанных с новыми информационными технологиями, разрабатывать инновационные методы и инструментальные средства для повышения информационной безопасности технологических платформ, систем и сервисов ИТ, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения, разрабатывать методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения, а также владеющих нормативными и правовыми основами в сфере информационной безопасности.

Планируемые результаты освоения образовательной программы

Универсальные, общепрофессиональные и профессиональные компетенции, формирующие академическую и практическую составляющие результатов освоения, предусмотренные образовательной программой, являются обязательными для освоения вне зависимости от особенностей индивидуальной образовательной траектории. Универсальные и общепрофессиональные компетенции наследуются из ФГОС для ФИИТ¹⁰. Ниже рассмотрим профессиональные компетенции профиля.

Профессиональные компетенции профиля

Компетенции/навыки:

ПК 1. Способен понимать и применять на практике гуманитарные, организационные и нормативные аспекты кибербезопасности, включая:

- методы управления рисками и методики оценки рисков,
- методы управления непрерывностью бизнеса и реагирования на инциденты,
- методики восстановления функционирования систем ИТ,
- правовые основы защиты информации, юридические аспекты информационной безопасности,
- методы, механизмы и сервисы защиты данных,
- методы средства обнаружения злоумышленных действий в киберпространстве,
- принципы защиты интеллектуальной собственности,
- методы обеспечения осведомленности и понимания ИБ внутри организации,
- принципы конфиденциальности персональных данных,
- методы и технологии защиты конфиденциальной информации.

ПК 2. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с выявлением вредоносных программ (ВП), вирусов и других атакующих технологий, а также обеспечением защиты активов и процессов от атакующих технологий и сущностей, включая:

- классификацию ВП и вирусов, методы определения их характерных особенностей,
- методы выявления вирусов и обнаружения ВП, моделирования кибератак, прогнозирования последствий исполнения вредоносных воздействий,
- методы и средства статического и динамического анализа ВП и защиты от вредоносного ПО,
- методы и средства моделирования поведения атакующей роли (противника) и определения характеристик хакера,
- методы и средства обнаружения инцидентов, разработки моделей управления инцидентами, выбора способов защиты от кибератак,
- методы и средства анализа данных о событиях ИБ и расследования инцидентов методами криминалистического моделирования и анализа,
- методы и средства обработки инцидентов, восстановления состояния после инцидента, реализации превентивных и контрмер, оценки эффективности управления инцидентами,
- методы управления инцидентами, связанными с человеческим фактором.
- методы анализа устойчивости моделей машинного обучения к атакам и обеспечения робастности моделей машинного обучения.

ПК 3. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с обеспечением и информационной защитой систем ИТ, включая:

- математические основы криптографии,
- модели, методы и протоколы криптографической защиты информации,
- теоретические основы, методы и стандарты симметричного шифрования, протоколы аутентификации на основе

¹⁰ ФГОС ВО – бакалавриат по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии: утв. приказом Министерства образования и науки Российской Федерации 12 марта 2015 г. № 224 [Электронный ресурс]. URL: <http://fgosvo.ru/uploadfiles/fgosvob/020302.pdf> (дата обращения: 24.07.2021).



- использования симметричных алгоритмов,
- теоретические основы, методы и стандарты криптосистем с открытым ключом,
 - методы и стандарты электронной подписи,
 - протоколы аутентификации на основе использования схем электронной подписи и криптосистем с открытым ключом,
 - модели типовых атак и модель противника,
 - принципы проектирования безопасных операционных систем (ОС) и основных механизмов ИБ в ОС,
 - принципы обеспечения ИБ при использовании виртуальных машин и гипервизоров,
 - методы анализа уязвимостей распределенных систем,
 - методы анализ уязвимостей распределенных баз данных,
 - проблемы ИБ и методы их решений для кластеров,
 - методы, алгоритмы и средства защиты от киберугроз систем, построенных с использованием методов искусственного интеллекта и машинного обучения,
 - протоколы аутентификации и авторизации: уязвимости и их последствия.
- ПК 4. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с разработкой безопасного программного обеспечения (ПО) и безопасных веб-платформ, включая:
- методы разработки моделей жизненного цикла безопасного ПО (ЖЦ БПО),
 - методы определения целей, стратегии и политики безопасности (информационной, функциональной, технологической) для БПО,
 - методы оценка активов и анализа рисков уязвимостей ПО на протяжении ЖЦ БПО,
 - меры, методы и средства, предназначенные для обеспечения безопасности ПО на протяжении ЖЦ БПО,
 - методы и средства тестирования безопасности и восстановления ПО,
 - методы анализа уязвимости сущностей Web&Mobile-экосистемы: приложений, веба, магазина приложений, провайдеров услуг, средств связи сущностей экосистемы: интерфейсов, механизмов аутентификации и управления доступом, протоколов PKI и HTTPS, X.509, cookies,
 - классификацию фишинговых атак, методы выявления уязвимостей хранения данных и физических уязвимостей на стороне клиента, способы противодействия атакам на стороне клиента,
 - классификацию уязвимостей и видов атак на стороне сервера, способы противодействия атакам на стороне сервера,
 - политику управления паролями, методы генерации и оценки паролей.
- ПК 5. Способен понимать и применять на практике методы и средства кибербезопасности, связанные с безопасностью инфраструктуры (сетевых технологий, аппаратных средств, киберфизических систем, телекоммуникационных систем), включая:
- модели сетевых архитектур с протоколами сетевой безопасности, функциональные возможности протоколов сетевой безопасности,
 - классификацию и назначение протоколов сетевой безопасности сети интернет,
 - классификацию уязвимостей протоколов прикладного уровня сети интернет и методы их обнаружения и защиты,
 - методы обеспечения защиты системы DNS,
 - методы обеспечения защиты протокола HTTP,
 - способы установления безопасного транспортного соединения, методы формирования главного секрета и общих ключей для транспортного соединения, безопасной передачи данных по протоколу TLS,
 - архитектуру и протоколы инфраструктуры открытого ключа (PKI),
 - методы обеспечения безопасности для протоколов сетевого уровня IPv6 и IPv4, протокол IPsec (IKEv2, ESP),
 - методы безопасности для протокола маршрутизации и протоколов канального уровня,
 - архитектуру, принципы функционирования и защиты программно-коммутируемых сетей (SDN),
 - методы обеспечения безопасности и защиты беспроводных локальных сетей,
 - методы обеспечения безопасности и защиты сетевых технологий Интернета вещей,
 - методы обеспечения безопасности и защиты файрволов пакетов и шлюзов прикладного уровня,
 - принципов создания и функционирования систем обнаружения и предотвращения проникновений в сетевую инфраструктуру,
 - классификацию уровней аппаратной безопасности (У-диаграмма Гайски и Куна), концепция корня доверия и моделей угроз в контексте безопасности оборудования,
 - методы оценки ИТ-продуктов на основе международного стандарта ISO / IEC 15408 (Общие критерии оценки безопасности информационных технологий),
 - принципы концепции безопасных и доверенных платформ (Trusted Platform),
 - принципы аппаратной реализации криптографических алгоритмов,
 - методы и средства защиты кибер-физических систем (CPS) от естественных и искусственных угроз, включая средства информационной безопасности,
 - фундаментальные концепции и основные методы и средства в беспроводной связи для обеспечения конфиденциальности, целостности, управления доступом и скрытой связи,
 - методы обеспечения устойчивой к помехам связи,
 - методы и средства обеспечения безопасности физического уровня выбранных коммуникационных технологий,
 - российские стандарты и рекомендации по стандартизации в области протоколов криптографической защиты информации: порядок применения криптографических алгоритмов ГОСТ в протоколах TLS 1.2, TLS 1.3, IPsec.

Заключение

Основная цель статьи состояла в том, чтобы ознакомить профессиональное сообщество с общими характеристиками разработанного автором профиля «Кибербезопасность и искусственный интеллект» для направления подготовки 02.03.02 Фундаментальная информатика и информационные техно-



логии. В частности, в статье рассмотрены: назначение, цели и профессиональные компетенции как ожидаемые результаты обучения по данному профилю.

Создание данного профиля явилось заключительным этапом выполненного под руководством автора с группой студентов кафедры информационной безопасности ВМК МГУ проекта по исследованию системы цифровых навыков кибербезопасности. Результатом первого этапа стала разработка модели цифровых навыков кибербезопасности [6], на втором этапе был разработан свод знаний кибербезопасности, на основе МНК¹¹ и куррикулум кибербезопасности [24]. Создание профиля «Кибербезопасность и искусственный интеллект» осуществлялось на основе результатов, полученных на предыдущих этапах проекта. В статье также мотивируется выбор в качестве базового направления подготовки направления ФИИТ, изначально созданного как многопрофильный стандарт, ориентированный на подготовку ИТ-специалистов по широкому спектру ИТ-направлений. Отмечается, что ФИИТ отвечает современным тенденциям развития области ИТ и ИТ-образования, в частности, духу документов Computing Curricula 2005 и Computing Curricula 2020 [25].

Список использованных источников

- [1] Computing as a discipline / D. E. Comer, D. Gries, M. C. Mulder [и др.]. – DOI 10.1145/63238.63239 // Communications of the ACM. – 1989. – Vol. 32, issue 1. – Pp. 9-23.
- [2] Сухомлин, В. А. Международные образовательные стандарты в области информационных технологий / В. А. Сухомлин // Прикладная информатика. – 2012. – № 1(37). – С. 33-54. – URL: <https://elibrary.ru/item.asp?id=17363662> (дата обращения: 15.07.2021). – Рез. англ.
- [3] Sukhomlin, V. Analytical Review of the Current Curriculum Standards in Information Technologies / V. Sukhomlin, E. Zubareva. – DOI 10.1007/978-3-030-46895-8_1 // Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science; ed. by V. Sukhomlin, E. Zubareva. – Springer, Cham. – 2020. – Vol. 1201. – Pp. 3-41.
- [4] Sukhomlin, V. Multiplatform System of Digital Talents Development "Academy of OIT" / V. Sukhomlin, E. Zubareva, D. Namiot. – DOI 10.1007/978-3-030-78273-3_1 // Modern Information Technology and IT Education. SITITO 2017. Communications in Computer and Information Science; ed. by V. Sukhomlin, E. Zubareva. – Springer, Cham. – 2021. – Vol. 1204. – Pp. 3-13.
- [5] Терехов, А. А. Computing Curricula: Software Engineering и российское образование / А. А. Терехов, А. Н. Терехов // Открытые системы. СУБД. – 2006. – № 8. – С. 61-66. – URL: <https://www.elibrary.ru/item.asp?id=12887260> (дата обращения: 24.07.2021).
- [6] Модель цифровых навыков кибербезопасности 2020 / В. А. Сухомлин, О. С. Белякова, А. С. Климина [и др.]. – DOI 10.25559/SITITO.16.202003.695-710 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 3. – С. 695-710. – Рез. англ.
- [7] Архитектура и принципы разработки куррикулума для дисциплины «Кибербезопасность» / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, Е. В. Зубарева, А. В. Якушин. – DOI 10.25559/SITITO.16.202004.927-939 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 4. – С. 927-939. – Рез. англ.
- [8] Система развития цифровых навыков ВМК МГУ & Базальт СПО: Методика классификации и описания требований к сотрудникам и содержанию образовательных программ в сфере информационных технологий / В. А. Сухомлин, Е. В. Зубарева, Д. Е. Намиот, А. В. Якушин. – DOI 10.29003/m2575.978-5-317-06336-8. – М.: МАКС Пресс, 2021. – 184 с. – URL: <https://www.elibrary.ru/item.asp?id=47887286> (дата обращения: 24.07.2021).
- [9] Сухомлин, В. А. Методологические аспекты концепции цифровых навыков / В. А. Сухомлин, Е. В. Зубарева, А. В. Якушин. – DOI 10.25559/SITITO.2017.2.253 // Современные информационные технологии и ИТ-образование. – 2017 – Т. 13, № 2 – С. 146-152. – Рез. англ.
- [10] Модель цифровых навыков кибербезопасности / В. А. Сухомлин, О. С. Белякова, А. С. Климина [и др.]. – DOI 10.25559/e3858-3795-1033-h. – М.: Фонд Лига интернет-медиа, 2021. – 294 с. – URL: <https://www.elibrary.ru/item.asp?id=46461613> (дата обращения: 24.07.2021). – Рез. англ.
- [11] Clear, A. Designing Computer Science Competency Statements: A Process and Curriculum Model for the 21st Century / A. Clear [и др.]. – DOI 10.1145/3437800.3439208 // Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education (ITiCSE-WGR '20). – Association for Computing Machinery, New York, NY, USA, 2020. – Pp. 211-246.
- [12] Cybersecurity education: Evolution of the discipline and analysis of master programs / K. Cabaj, D. Domingos, Z. Kotulski, A. Respicio. – DOI 10.1016/j.cose.2018.01.015 // Computers & Security. – 2018. – Vol. 75. – Pp. 24-35.
- [13] Global perspectives on cybersecurity education / A. Parrish, J. Impagliazzo, R. K. Raj [и др.]. – DOI 10.1145/3197091.3205840 // Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018). – Association for Computing Machinery, New York, NY, USA, 2018. – Pp. 340-341.
- [14] Hawthorne, E. K. Multifarious initiatives in cybersecurity education / E. K. Hawthorne. – DOI 10.1145/2505990.2505999 // ACM Inroads. – 2013. – Vol. 4, issue 3. – Pp. 46-47.
- [15] Cybersecurity knowledge and skills taught in capture the flag challenges / V. Švábenský, P. Čeleda, J. Vykopal, S. Brišáková. – DOI 10.1016/j.cose.2020.102154 // Computers & Security. – 2021. – Vol. 102. – Article number: 102154.
- [16] Cybersecurity Education: The Skills Gap, Hurdle! / S. N. John, E. Noma-Osaghae, F. Oajide, K. Okokpuije. – DOI 10.1007/978-3-030-50244-7_18 // Innovations in Cyber-

¹¹ CyBok: The Cyber Security Body of Knowledge / ed. by A. Rashid [и др.]. Version 1.0. 31st October, 2019. National Cyber Security Centre, 2019. [Электронный ресурс]. URL: <https://www.cybok.org> (дата обращения: 24.07.2021).



- security Education; ed. by K. Daimi, G. Francia. – Springer, Cham, 2020. – Pp. 361-376.
- [17] Hodson, C. *Cybersecurity Skills* / C. Hodson. – DOI 10.1007/978-3-642-27739-9_1577-1 // *Encyclopedia of Cryptography, Security and Privacy*; ed. by S. Jajodia, P. Samarati, M. Yung. – Springer, Berlin, Heidelberg, 2020.
- [18] Wang, P. *A Comprehensive Mentoring Model for Cybersecurity Education* / P. Wang, R. Sbeit. – DOI 10.1007/978-3-030-43020-7_3 // *17th International Conference on Information Technology – New Generations (ITNG 2020). Advances in Intelligent Systems and Computing*; ed. by S. Latifi. – Springer, Cham, 2020. – Vol. 1134. – Pp. 17-23.
- [19] Ghernaouti, S. *Research and Education as Key Success Factors for Developing a Cybersecurity Culture* / S. Ghernaouti, B. Wanner. – DOI 10.1007/978-3-658-21655-9_38 // *Cybersecurity Best Practices*; ed. by M. Bartsch, S. Frey. – Springer Vieweg, Wiesbaden, 2018. – Pp. 539-552.
- [20] *The Impact of Changing Technology on International Cybersecurity Curricula* / H. Read, I. Sutherland, K. Xynos [и др.]. – DOI 10.1007/978-3-319-58460-7_36 // *Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science*; ed. by T. Tryfonas. – Springer, Cham, 2017. – Vol. 10292. – Pp. 518-528.
- [21] Blair, J. R. S. *Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum* / J. R. S. Blair, C. M. Chewar, R. K. Raj, E. Sobiesk. – DOI 10.1145/3341525.3387426 // *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20)*. – Association for Computing Machinery, New York, NY, USA, 2020. – Pp. 82-88.
- [22] *Enhancing interest in cybersecurity careers: a peer mentoring perspective* / V. P. Janeja [и др.]. – DOI 10.1145/3159450.3159563 // *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. – Association for Computing Machinery, New York, NY, USA, 2018. – Pp. 384-389.
- [23] *Realism in Teaching Cybersecurity Research: The Agile Research Process* / M. Dark [и др.]. – DOI 10.1007/978-3-319-18500-2_1f // *Proceedings of the 9th IFIP World Conference on Information Security Education (WISE)*. – Hamburg, Germany, 2015. – Pp. 3-14.
- [24] *Куррикулум дисциплины «Кибербезопасность»* / В. А. Сухомлин, С. В. Лебедь, О. С. Белякова [и др.]. – DOI 10.25559/f6676-8117-2920-j. – М.: Фонд «Лига интернет-медиа», 2022. – 402 с. – Рез. англ.
- [25] Frezza, S. *Modeling global competencies for computing education* / S. Frezza, A. Pears, M. Daniels [и др.]. – DOI 10.1145/3197091.3205844 // *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*. – Association for Computing Machinery, New York, NY, USA, 2018. – Pp. 348-349.

Поступила 24.07.2021; одобрена после рецензирования 25.08.2021; принята к публикации 04.09.2021.

Об авторе:

Сухомлин Владимир Александрович, заведующий лабораторией открытых информационных технологий, факультет вычислительной математики и кибернетики, ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (119991, Российская Федерация, г. Москва, ГСП-1, Ленинские горы, д. 1), доктор технических наук, профессор, **ORCID: <https://orcid.org/0000-0001-9468-7138>**, sukhomlin@mail.ru

Автор прочитал и одобрил окончательный вариант рукописи.

References

- [1] Comer D.E., Gries D., Mulder M.C., Tucker A., Turner A.J., Young P.R., Denning P.J. Computing as a discipline. *Communications of the ACM*. 1989; 32(1):9-23. (In Eng.) DOI: <https://doi.org/10.1145/63238.63239>
- [2] Sukhomlin V.A. Educational Standards in the Field of Information Technologies. *Journal of Applied Informatics*. 2012; (1):33-54. Available at: <https://elibrary.ru/item.asp?id=17363662> (accessed 24.07.2021). (In Russ., abstract in Eng.)
- [3] Sukhomlin V., Zubareva E. Analytical Review of the Current Curriculum Standards in Information Technologies. In: Ed. by V. Sukhomlin, E. Zubareva. *Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science*. 2020; 1201:3-41. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-46895-8_1
- [4] Sukhomlin V., Zubareva E., Namiot D. Multiplatform System of Digital Talents Development "Academy of OIT". In: Ed. by V. Sukhomlin, E. Zubareva. *Modern Information Technology and IT Education. SITITO 2017. Communications in Computer and Information Science*. 2021; 1204:3-13. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-78273-3_1
- [5] Terekhov A.A., Terekhov A.N. Computing Curricula: Software Engineering and Russian Education. *Open Systems.DBMS*. 2006; (8):61-66. Available at: <https://www.elibrary.ru/item.asp?id=12887260> (accessed 24.07.2021). (In Russ.)
- [6] Sukhomlin V.A., Belyakova O.S., Klimina A.S., Polyanskaya M.S., Rusanov A.A. Cybersecurity Digital Skills Model 2020. *Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education*. 2020; 16(3):695-710. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.16.202003.695-710>
- [7] Sukhomlin V.A., Belyakova O.S., Klimina A.S., Polyanskaya M.S., Zubareva E.V., Yakushin A.V. Architecture and Principles of Developing a Curriculum for the Academic Subject "Cybersecurity". *Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education*. 2020; 16(4):927-939. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.16.202004.927-939>
- [8] Sukhomlin V.A., Zubareva E.V., Namiot D.E., Yakushin A.V. *Sistema razvitija cifrovyyh navykov VMK MGU & Bazal't SPO. Metodika klassifikacii i opisaniya trebovanij k sotrudnikam i soderzhani obrazovatel'nyh programm v sfere informacionnyh tehnologii* [System for the Development of Digi-



- tal Skills MSU Faculty of Computational Mathematics and Cybernetics & BaseALT]. Moscow, MAKS Press, BaseALT; 2021. 184 p. (In Russ.) DOI: <https://doi.org/10.29003/m2575.978-5-317-06336-8>
- [9] Sukhomlin V.A., Zubareva E.V., Yakushin A.V. Methodological Aspects of the Digital Skills Concept. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2017; 13(2):146-152. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/SITITO.2017.2.253>
- [10] Sukhomlin V.A., Belyakova O.S., Klimina A.S., Polyanskaya M.S., Rusanov A.A. *Model' cifrovyyh navykov kiberbezopasnosti* [Cybersecurity Digital Skills Model]. The League Internet Media Fund, Moscow; 2021. 294 p. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/e3858-3795-1033-h>
- [11] Clear A., et al. Designing Computer Science Competency Statements: A Process and Curriculum Model for the 21st Century. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education (ITiCSE-WGR '20)*. Association for Computing Machinery, New York, NY, USA; 2020. p. 211-246. (In Eng.) DOI: <https://doi.org/10.1145/3437800.3439208>
- [12] Cabaj K., Domingos D., Kotulski Z., Respicio A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*. 2018; 75:24-35. (In Eng.) DOI: <https://doi.org/10.1016/j.cose.2018.01.015>
- [13] Parrish A., Impagliazzo J., Raj R.K., Santos H., Asghar M.R., Jøsang A., Pereira T., Sá V.J., Stavrou E. Global perspectives on cybersecurity education. *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*. Association for Computing Machinery, New York, NY, USA; 2018. p. 340-341. (In Eng.) DOI: <https://doi.org/10.1145/3197091.3205840>
- [14] Hawthorne E.K. Multifarious initiatives in cybersecurity education. *ACM Inroads*. 2013; 4(3):46-47. (In Eng.) DOI: <https://doi.org/10.1145/2505990.2505999>
- [15] Švábenský V., Čeleda P., Vykopal J., Brišáková S. Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*. 2021; 102:102154. (In Eng.) DOI: <https://doi.org/10.1016/j.cose.2020.102154>
- [16] John S.N., Noma-Osaghae E., Oajide F., Okokpujie K. Cybersecurity Education: The Skills Gap, Hurdle! In: Ed. by K. Daimi, G. Francia. *Innovations in Cybersecurity Education*. Springer, Cham; 2020. p. 361-376. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-50244-7_18
- [17] Hodson C. Cybersecurity Skills. In: Ed. by S. Jajodia, P. Samarati, M. Yung. *Encyclopedia of Cryptography, Security and Privacy*. Springer, Berlin, Heidelberg; 2020. (In Eng.) DOI: https://doi.org/10.1007/978-3-642-27739-9_1577-1
- [18] Wang P., Sbeit R. A Comprehensive Mentoring Model for Cybersecurity Education. In: Ed. by S. Latifi. *17th International Conference on Information Technology - New Generations (ITNG 2020). Advances in Intelligent Systems and Computing*. 2020; 1134:17-23. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-030-43020-7_3
- [19] Ghernaouti S., Wanner B. Research and Education as Key Success Factors for Developing a Cybersecurity Culture. In: Ed. by M. Bartsch, S. Frey. *Cybersecurity Best Practices*. Springer Vieweg, Wiesbaden; 2018. p. 539-552. (In Eng.) DOI: https://doi.org/10.1007/978-3-658-21655-9_38
- [20] Read H., Sutherland I., Xynos K., Drange T., Sundt E. The Impact of Changing Technology on International Cybersecurity Curricula. In: Ed. by T. Tryfonas. *Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science*. 2017; 10292:518-528. Springer, Cham. (In Eng.) DOI: https://doi.org/10.1007/978-3-319-58460-7_36
- [21] Blair J.R.S., Chewar C.M., Raj R.K., Sobieski E. Infusing Principles and Practices for Secure Computing Throughout an Undergraduate Computer Science Curriculum. *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20)*. Association for Computing Machinery, New York, NY, USA; 2020. p. 82-88. (In Eng.) DOI: <https://doi.org/10.1145/3341525.3387426>
- [22] Janeja V.P., Faridee A.Z.M., Gangopadhyay A., Seaman C., Everhart A. Enhancing interest in cybersecurity careers: a peer mentoring perspective. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. Association for Computing Machinery, New York, NY, USA; 2018. p. 384-389. (In Eng.) DOI: <https://doi.org/10.1145/3159450.3159563>
- [23] Dark M., Bishop M., Linger R., Goldrich L. Realism in Teaching Cybersecurity Research: The Agile Research Process. *Proceedings of the 9th IFIP World Conference on Information Security Education (WISE)*. Hamburg, Germany; 2015. p. 3-14. (In Eng.) DOI: https://doi.org/10.1007/978-3-319-18500-2_1f
- [24] Sukhomlin V.A., Lebed S.V., Belyakova O.S. *Kurrikulum discipliny Kiberbezopasnost'* [Curriculum for the Discipline "Cybersecurity"]. The League Internet Media Fund, Moscow; 2022. 402 p. (In Russ., abstract in Eng.) DOI: <https://doi.org/10.25559/f6676-8117-2920-j>
- [25] Frezza S., Pears A., Daniels M., et al. Modeling global competencies for computing education. *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*. Association for Computing Machinery, New York, NY, USA; 2018. p. 348-349. (In Eng.) DOI: <https://doi.org/10.1145/3197091.3205844>

Submitted 24.07.2021; approved after reviewing 25.08.2021;
accepted for publication 04.09.2021.

About the author:

Vladimir A. Sukhomlin, Head of the Open Information Technologies Lab, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1 Leninskie gory, Moscow 119991, GSP-1, Russian Federation), Dr. Sci. (Tech.), Professor, **ORCID:** <https://orcid.org/0000-0001-9468-7138>, sukhomlin@mail.ru

The author has read and approved the final manuscript.

