Концепция и основные характеристики магистерской программы "Кибербезопасность" факультета ВМК МГУ

В.А. Сухомлин

Аннотация **– Статья посвящена описанию концепции и основных характеристик магистерской программы "Кибербезопасность", разработанной факультетом вычислительной математики и кибернетики МГУ имени М.В. Ломоносова совместно с Департаментом кибербезопасности ПАО Сбербанк. Рассмотрены цели, основные принципы разработки, архитектура свода знаний магистерской программы, ее принципиальные особенности, профессиональные компетенции как ожидаемые результаты обучения, состав дисциплин. Магистерская программа "Кибербезопасность" предназначена для тех, кто хочет получить глубокие знания и навыки в области информационной безопасности и защиты информации и данных от кибератак. Программа ориентирована на подготовку магистров науки по кибербезопасности. Она разработана в соответствии с современными международными профессиональными и образовательными стандартами и с учетом действующих национальных стандартов и норм.**

Ключевые слова **– Кибербезопасность, информационная безопасность, модель цифровых навыков кибербезопасности, куррикулум кибербезопасности, свод знаний кибербезопасности, архитектурная модель кибербезопасности, компетенции кибербезопасности, магистерская программа, ФИИТ.**

I. Введение

Всеобъемлющая цифровизация по существу всех сфер жизни и деятельности человека ведет к тому, что сектор информационных технологий (ИТ) становится системообразующим фактором в жизни социума, отдельных государств, каждого человека. Информационные системы, цифровые платформы, сетевые технологии, базы знаний, интеллектуальные сервисы и приложения играют центральную роль в управлении основополагающими системами жизнеобеспечения общества, функционирование которых уязвимо перед случайными и преднамеренными киберугрозами и целиком зависит от информационной безопасности используемых цифровых технологий.

Кибербезопасность – это как раз та область, которая занимается защитой от киберугроз, таких как вирусы, хакерские атаки, кибершпионаж и т.д., при этом актуальность кибербезопасности постоянно возрастает, так как киберугрозы становятся все более утонченными и сложными, что требует постоянного совершенствования технологий и методов защиты. Кибербезопасность является ключевым элементом в обеспечении работы предприятий критической инфраструктуры, таких как энергетические системы, транспортные сети и финансовые учреждения, нарушение информационной безопасности которых может привести к серьезным последствиям для экономики и безопасности страны. Актуальность области кибербезопасности определяется необходимостью защиты активов от киберугроз, сохранения конфиденциальности и целостности данных, а также обеспечения безопасного функционирования предприятий критической инфраструктуры.

Повышение уровня кибербезопасности активов и защита критически важных информационных инфраструктур имеют важное значение для безопасности и экономического благополучия каждой страны, особенно в условиях глобального движения к цифровой экономике и информационному обществу. Кибербезопасность является важным элементом системы национальной безопасности страны.

В связи с вышеизложенным востребованность в специалистах по кибербезопасности постоянно возрастает. Многие учебные учреждения и тренинговые центры предлагают курсы и программы подготовки специалистов того или иного уровня в области кибербезопасности.

Отличительной особенностью предлагаемой магистерской программы "Кибербезопасность" (далее Программа) является то, что она ориентирована на подготовку магистров науки по кибербезопасности, способных выполнять исследования в этой сфере, разрабатывать новые инструментальные средства для решения задач кибербезопасности, решать комплексные задачи информационной защиты активов и критических инфраструктур.

Программа разработана в соответствии с современными международными профессиональными и образовательными стандартами и с учетом действующих национальных стандартов и норм. Одним из важнейших

Статья получена 25 мая 2023.

Сухомлин Владимир Александрович, заведующий лабораторией открытых информационных технологий факультета 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 (e-mail: sukhomlin@mail.ru).

критериев разработки Программы и составляющих ее двух десятков дисциплин является возможно полное соответствие своду отраслевых знаний CyBOK (The Cyber Security Body of Knowledge).

II. Цель, принципы разработки, модель совместной магистерской программы

Цель создания совместной магистерской программы МГУ-СБЕР в области кибербезопасности состояла в том, чтобы разработать и внедрить в образовательную практику страны типовую магистерскую программу по кибербезопасности, предназначенную для подготовки специалистов высшей квалификации, владеющих современными научными знаниями и технологиями в области кибербезопасности и способных:

- выполнять научные исследования, связанные с кибербезопасностью для наиболее актуальных направлений ИТ, включая: системы искусственного интеллекта, распределенные вычисления, интернет вещей, индустриальный интернет, киберфизические системы, Большие данные, технологии блокчейн, метавселенная и др.;
- разрабатывать методы и инструментальные средства для решения актуальных задач кибербезопасности активов и систем, в том числе с применением методов и технологий искусственного интеллекта (ИИ);
- разрабатывать методы, алгоритмы и средства защиты от киберугроз систем искусственного интеллекта, анализировать устойчивость моделей машинного обучения к атакам и обеспечивать робастность моделей машинного обучения;
- создавать доверенные технологические платформы, системы и сервисы ИТ на основе методологии DevSecOps;
- решать комплексные задачи кибербезопасности систем и процессов критической инфраструктуры, а также процессов автоматизации социально-производственной деятельности.

Разработка Программы основывалась на предшествующих работах, выполненных автором и под его руководством. К ним, в частности, относятся:

- исследование и разработка модели цифровых навыков кибербезопасноти [1, 2],
- разработка куррикулума дисциплины «Кибербезопасность» [3, 4] (КК 2021),
- разработка профиля "Кибербезопасность и искусственный интеллект" по направлению подготовки 02.04.02 "Фундаментальная информатика и информационные технологии" (ФИИТ) [5, 6],
- исследование цифровых навыков кибербезопасности стандарта SFIA8 [7],
- исследование международной стандартизации системы ИТ-образования на новом этапе [8].

В указанных работах методологические принципы для разработки образовательных программ определялись посредством совместного анализа представлений кибербезопасности, рассматриваемой в трех следующих измерениях [2]:

- как области профессиональной деятельности, которая определяется на языке международных стандартов цифровых навыков, ролей и профилей;
- как обширной научно-прикладной области знаний и технологий, которая представляется в виде архитектурных моделей или таксономий кибербезопасности, а также стандартизованным сводом знаний (CyBoK 2019) и системой стандартов информационной безопасности;
- как сектор ИТ-образования, предназначенный для подготовки профессиональных кадров по кибербезопасности на основе стандартов куррикулумов [4].

На финишной стадии проекта в качестве базовых методологических руководств использовались:

- Куррикулум дисциплины «Кибербезопасность» или КК 2021 [3, 4] – использовалась архитектура свода знаний и содержание дисциплин кибербезопасности;
- CyBOK 2019 (The Cyber Security Body of Knowledge) [9] – использовался как наиболее полный справочник общепризнанных на международном уровне профессиональных знаний в области кибербезопасности.

Свод знаний кибербезопасности, представленный в CyBOK, организован в виде иерархической системы элементов знаний. Верхний уровень таксономии этой системы разделяется на следующие пять категорий:

- Человеческие, организационные и нормативные аспекты (Human, Organisational, and Regulatory Aspects)
- Атаки и Защита (Attacks and Defences)
- Безопасность систем (Systems Security)
- Безопасность программного обеспечения и платформ (Software and Platform Security)
- Безопасность инфраструктуры (Infrastructure Security).

По сравнению с CyBoK в архитектуру свода знаний КК 2021 введена дополнительно категория «Безопасность технологий экосистемы» (представленная в Программе дисциплиной «Безопасность инфраструктурных технологий»), ориентированная на проблематику информационной безопасности таких инфраструктурных технологий экосистемы как, интернет вещей, индустриальный интернет, киберфизические системы, Большие данные, технологии блокчейн.

Также в архитектуру КК2021 включены категории базовой (бакалаврской) подготовки, которые рассматриваются как желательный бэкграунд учащихся магистерской программы «Кибербезопасность»:

1. Базовые навыки компьютерных наук (Computer Science).
2. Математика для кибербезопасности (Cybersecurity math).
3. Менеджмент проектов и системы менеджмента качества (Project management and quality management systems).
4. Универсальные трудовые и социально-личностные (мягкие) навыки (Soft skills).

Архитектура свода знаний КК2021 показана на рисунке 1.

Формирование магистерской программы "Кибербезопасность" основывалось на следующих принципах.

1. Возможно более полное отражение в содержании Программы объема знаний, определенного в CyBoK.
2. Преимущественное включение в Программу наукоемких дисциплин, обладающих научной перспективой при их реализации в университетском окружении.

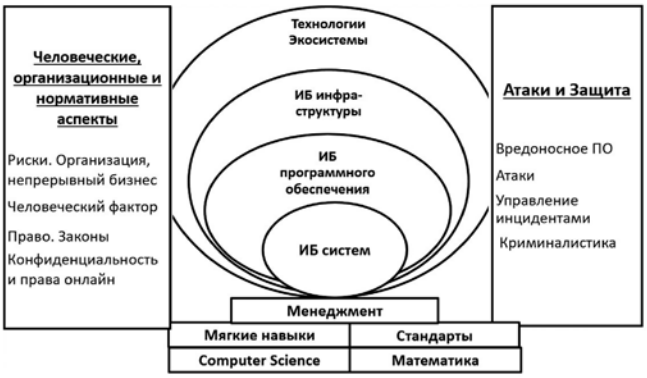

Рис. 1. Архитектура свода знаний куррикулума дисциплины "Кибербезопасность" или КК 2021, в основании которой указаны категории базовых знаний, рассматриваемых как бэкграунд для освоения магистерской программы "Кибербезопасность" [1, С. 704]

3. Формирование содержания дисциплин на основе содержания соответствующих разделов CyBoK.
4. Введение в Программу в качестве базовой методологической дисциплины "Системной инженерии" с акцентом на моделебазированный подход, использование языков моделирования и поддержки SecDevOps методологий.
5. Включение углубленного двухсеместрового курса по криптографии, дополненного дисциплиной "Постквантовой криптографии" (по выбору).
6. Включение в Программу дисциплины "Искусственный интеллект в кибербезопасности", посвященной методам, алгоритмам и средствам защиты от киберугроз систем искусственного интеллекта, анализу устойчивости моделей машинного обучения к атакам [10].
7. Включение в Программу дисциплины "Безопасность инфраструктурных технологий", посвященной вопросам кибербезопасности интернета вещей и индустриального интернета, киберфизических систем, Больших данных, технологий блокчейн [11].
8. Введение в свод знаний новой категории "Операционная деятельность", включающей набор критически важных наукоемких дисциплин для решения научных и прикладных задач в области кибербезопасности предприятий критической инфраструктуры (в частности дисциплины: Технологии больших данных, Аналитика больших данных, Искусственный интеллект в кибербезопасности, Безопасность инфраструктурных технологий), а также практико-ориентированные дисциплины по профилю деятельности базовой организации.
9. Введение в Программу практико-ориентированных курсов "Центр киберзащиты: функции, процессы, технологии" и "Практика противоборства кибератакам", реализуемых на производственной базе партнера – Департамента кибербезопасности ПАО Сбербанк[1] [12].

В Таблице I показано соответствие категорий и дисциплин в магистерской программе "Кибербезопасность".

Таблица I
Соответствие категорий и дисциплин в магистерской программе "Кибербезопасность"

Категории свода знаний	**Дисциплины**
Атаки и Защита	Вредоносное ПО и средства защиты Операции ИБ и управление инцидентами
Безопасность систем	Основы криптографии Безопасность ОС и виртуализации Безопасность распределенных систем Постквантовая криптография
Безопасность программного обеспечения и платформ	Безопасность программного обеспечения Безопасность веб-платформ и сервисов
Безопасность инфраструктуры	Безопасность компьютерных сетей Безопасность интернет-технологий Безопасность аппаратного уровня
Безопасность технологий экосистемы	Безопасность инфраструктурных технологий
Человеческие, организационные и нормативные аспекты	Нормативно-правовое обеспечение и аудит кибербезопасности Менеджмент риска информационной безопасности
Операционная деятельность	Системная инженерия + семинар Технологии больших данных Аналитика больших данных Искусственный интеллект в кибербезопасности Центр киберзащиты: функции, процессы, технологии (на производственной базе Департамента кибербезопасности ПАО Сбербанк) Практика противоборства кибератакам (на производственной базе Департамента кибербезопасности ПАО Сбербанк)

Модель Программы представлена на рисунке 2.

[1] Валуйских С. А. Второй SOC Сбербанка [Электронный ресурс] // BIS Journal. 2018. № 3(30). URL: https://ib-bank.ru/bisjournal/post/689 (дата обращения: 25.05.2023).

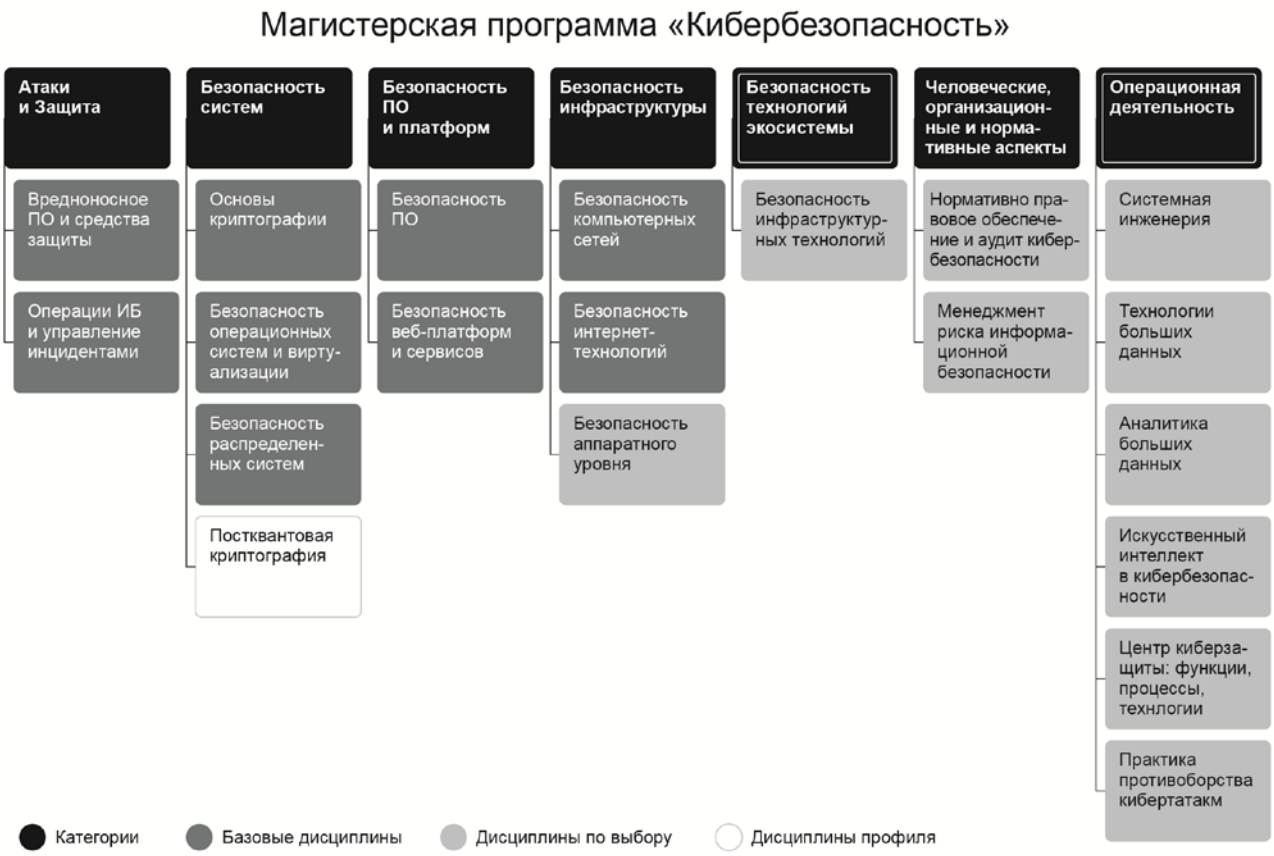

Рис. 2. Модель магистерской программы "Кибербезопасность"

В модели Программы для целей учебного менеджмента выделены цветом три класса дисциплин:

- базовые дисциплины (Вредоносное ПО и средства защиты, Операции ИБ и управление инцидентами, Основы криптографии, Безопасность ОС и виртуализации, Безопасность программного обеспечения, Безопасность компьютерных сетей, Безопасность интернет-технологий, Безопасность веб-платформ и сервисов);
- профильные дисциплины (Нормативно-правовое обеспечение и аудит кибербезопасности, Менеджмент риска информационной безопасности, Технологии больших данных, Аналитика больших данных, Безопасность инфраструктурных технологий, Искусственный интеллект в кибербезопасности, Центр киберзащиты: функции, процессы, технологии (на производственной базе Департамента кибербезопасности ПАО Сбербанк), Безопасность аппаратного уровня, Практика противоборства кибератакам (на производственной базе Департамента кибербезопасности ПАО Сбербанк);
- дисциплины по выбору (Постквантовая криптография и ряд дисциплин базового образования).

Кроме рассмотренных выше дисциплин Программа предполагает выполнение достаточно объемного научного исследования и написания магистерской диссертации (отводится примерно 2000 часов). Промежуточным этапом работы над диссертацией является курсовая работа (второй семестр) – суть которой составляет аналитический обзор по теме диссертации уровня журнальной статьи. Кроме этого, в течение четырех семестров в рамках Программы работает научный кафедральный семинар, как правило, дополненный просеминарами по отдельным темам, которые ведут научные руководители магистерских диссертаций.

III. Планируемые результаты освоения образовательной Программы

Методическое обеспечение в сфере образования предполагает определение планируемых результатов освоения образовательных программ в форме профессиональных компетенций.

Ниже определяется набор основных профессиональных компетенций, которые можно рассматривать как ожидаемые результаты подготовки по рассмотренной в данной статье Программе.

1. Знание основных понятий, принципов и методов кибербезопасности, включая анализ угроз, уязвимостей и рисков, а также методы защиты активов, данных и систем.

2. Умение проводить аудит и оценку уязвимостей активов, информационных систем и сетей, а также разрабатывать и реализовывать меры и средства по их защите.

3. Знание методов и средств криптографии и аутентификации, а также умение применять их для обеспечения конфиденциальности и целостности информации.

4. Умение проводить исследования в области кибербезопасности, анализировать и обобщать полученные данные, разрабатывать рекомендации, методы и средства для повышения эффективности информационной безопасности.

5. Умение работать с различными средствами и технологиями защиты информации, включая антивирусные программы, брандмауэры, VPN, IDS/IPS и другие.

6. Владение методами системной инженерии, языками моделирования, методологиями поддержки безопасного жизненного цикла продуктов и систем.

7. Владение методами и средствами защиты от киберугроз систем искусственного интеллекта, включая методы анализа устойчивости моделей машинного обучения к атакам.

8. Знание методов и технологий кибербезопасности для интернета вещей, киберфизических систем, Больших данных, технологий блокчейн.

9. Умение решать научные и прикладные задачи в области кибербезопасности предприятий критической инфраструктуры.

10. Знание методов и средств инцидентного управления и реагирования на кибератаки, а также умение разрабатывать и реализовывать планы действий в случае инцидентов.

11. Знание законодательных и нормативных актов в области кибербезопасности, а также умение применять их на практике.

IV. Заключение

В статье приводится описание концепции и основных характеристик магистерской программы "Кибербезопасность", разработанной факультетом вычислительной математики и кибернетики МГУ имени М.В. Ломоносова совместно со специалистами Департамента кибербезопасности ПАО Сбербанк под научным руководством автора. В статье сформулированы цели и основные принципы разработки, описана архитектура свода знаний магистерской программы и представлена ее модель, а также состав входящих в нее дисциплин. В заключении приведен список профессиональных компетенций как ожидаемых результаты обучения по данной программе.

Магистерская программа "Кибербезопасность" предназначена для тех, кто хочет получить глубокие знания и навыки в области информационной безопасности и защиты информации и данных от кибератак. Программа ориентирована на подготовку магистров науки по кибербезопасности. Итоговым результатом обучения по данной программе является защищенная магистерская диссертация. Программа разработана в соответствии с современными международными профессиональными и образовательными стандартами и с учетом действующих национальных стандартов и норм. Программа начинает реализовываться на факультете вычислительной математики и кибернетики Московского университета с 1 сентября 2023 года[2].

Библиография

[1] Модель цифровых навыков кибербезопасности 2020 / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, А. А. Русанов // Современные информационные технологии и ИТ-образование. 2020. Т. 16, № 3. С. 695-710. doi: https://doi.org/10.25559/SITITO.16.202003.695-710

[2] Модель цифровых навыков кибербезопасности / В. А. Сухомлин, О. С. Белякова, А. С. Климина [и др.]. М. : Фонд "Лига интернет-медиа", 2021. 294 с. doi: https://doi.org/10.25559/e3858-3795-1033-h

[3] 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 // Современные информационные технологии и ИТ-образование. 2020. Т. 16, № 4. С. 927-939. doi: https://doi.org/10.25559/SITITO.16.202004.927-939

[4] Куррикулум дисциплины "Кибербезопасность" / В. А. Сухомлин, С. В. Лебедь, О. С. Белякова, А. С. Климина, М. С. Полянская. М. : Фонд "Лига интернет-медиа", 2022. 402 с. doi: https://doi.org/10.25559/f6676-8117-2920-j

[5] Сухомлин, В. А. Создание профиля "Кибербезопасность и искусственный интеллект" для направления подготовки ФИИТ на основе куррикулумного подхода // Современные информационные технологии и ИТ-образование. 2021. Т. 17, № 3. С. 724-734. doi: https://doi.org/10.25559/SITITO.17.202103.724-734

[6] Сухомлин, В. А., Сухомлин, В. В. Концепция нового образовательного направления // Открытые системы. СУБД. 2003. № 02. URL: https://www.osp.ru/os/2003/02/182628

[7] Белякова, О. С., Сухомлин, В. А. Исследование навыков кибербезопасности стандарта SFIA8 // International Journal of Open Information Technologies. 2022. Т. 10, № 7. С. 156-193. URL: https://elibrary.ru/item.asp?id=49176177

[8] Сухомлин, В. А., Зубарева, Е. В. Новый этап международной стандартизации ИТ-образования // Современные информационные технологии и ИТ-образование. 2021. Т. 17, № 3. С. 697-723. doi: https://doi.org/10.25559/SITITO.17.202103.697-723

[9] Carolina, R. Law and Regulation Knowledge Area // CyBOK: Cyber Security Body of Knowledge ; ed. by A. Rashid, H. Chivers, G. Danezis, E. Lupu, A. Martin. Version 1.0. The National Cyber Security Centre, 2019. p. 49-144. URL: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

[10] Ильюшин, Е. А., Намиот, Д. Е., Чижов, И. В. Атаки на системы машинного обучения – общие проблемы и методы // International Journal of Open Information Technologies. 2022. Т. 10, № 3. С. 17-22. URL: https://elibrary.ru/item.asp?id=48102861

[11] Намиот, Д. Е., Сухомлин, В. А. О кибербезопасности систем Интернета Вещей // International Journal of Open Information Technologies. 2023. Т. 11, № 2. С. 85-97. URL: https://www.elibrary.ru/item.asp?id=50271028

[12] Лебедь, С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 383-390. doi: https://doi.org/10.25559/SITITO.18.202202.383-390

[2] Запуск магистерской программы "Кибербезопасность" : сайт ВМК МГУ [Электронный ресурс]. URL: https://cs.msu.ru/news/3916 (дата обращения: 25.05.2023).

The Concept and Main Characteristics of the Master's Degree Program "Cybersecurity" of the Faculty of Computational Mathematics and Cybernetics of Lomonosov Moscow State University

Vladimir A. Sukhomlin

***Abstract* – The article deals with the description of the concept and main characteristics of the Master's Degree Program "Cybersecurity", developed by the Faculty of Computational Mathematics and Cybernetics of Lomonosov Moscow State University together with the Cybersecurity Department of Sberbank of Russia PJSC. The objectives, the main principles of development, the architecture of the body of knowledge of the Master's Degree Program, its fundamental features, professional competencies as expected learning outcomes, and the composition of disciplines are considered. The Master's Degree Program "Cybersecurity" is intended for those who want to gain in-depth knowledge and skills in the field of information security and the protection of information and data from cyber attacks. The Program is focused on the training of Masters of Science in Cybersecurity. It was developed in accordance with modern international professional and educational standards and is based on existing national standards and norms.**

***Keywords* – Cybersecurity, Information Security, Cybersecurity Digital Skills Model, Cybersecurity Curriculum, Cybersecurity Body of Knowledge, Cybersecurity Architectural Model, Cybersecurity Competences, Master's Degree Program, FIIT (Fundamental Informatics and Information Technology).**

REFERENCES

[1] V. A. Sukhomlin, O. S. Belyakova, A. S. Klimina, M. S. Polyanskaya, and A. A. Rusanov, "Cybersecurity Digital Skills Model 2020," *Modern Information Technologies and IT-Education*, vol. 16, no. 3, pp. 695-710, 2020. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/SITI-TO.16.202003.695-710

[2] V. A. Sukhomlin, O. S. Belyakova, A. S. Klimina, M. S. Polyanskaya, and A. A. Rusanov, *Cybersecurity Digital Skills Model*. Moscow: Foundation "League of Internet Media", 2021. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/e3858-3795-1033-h

[3] V. A. Sukhomlin, O. S. Belyakova, A. S. Klimina, M. S. Polyanskaya, E. V. Zubareva, and A. V. Yakushin, "Architecture and Principles of Developing a Curriculum for the Academic Subject "Cybersecurity", *Modern Information Technologies and IT-Education*, vol. 16, no. 4, pp. 927-939, 2020. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/SITITO.16.202004.927-939

[4] V. A. Sukhomlin, S. V. Lebed, O. S. Belyakova, A. S. Klimina, and M. S. Polyanskaya, *Curriculum for the Discipline "Cybersecurity"*. Moscow: Foundation "League of Internet Media", 2022. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/f6676-8117-2920-j

[5] V. A. Sukhomlin, "Creating a Profile "Cybersecurity and Artificial Intelligence" for the Direction of FIIT Training Based on the Curriculum Approach," *Modern Information Technologies and IT-Education*, vol. 17, no. 3, pp. 724-734, 2021. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/SITITO.17.202103.724-734

[6] V. A. Sukhomlin, and V. V. Sukhomlin, "The concept of a new educational direction," *Open Systems. DBMS*, no. 02, 2003. [Online]. Available: https://www.osp.ru/os/2003/02/182628

[7] O. S. Belyakova, and V. A. Sukhomlin, "SFIA8 Cybersecurity Skills Study," *International Journal of Open Information Technologies*, vol. 10, no. 7, pp. 156-193, 2022. [Online]. Available: https://elibrary.ru/item.asp?id=49176177 (In Russ., abstract in Eng.)

[8] V. A. Sukhomlin, and E. V. Zubareva, "The New Stage of International Standardization of IT Education," *Modern Information Technologies and IT-Education*, vol. 17, no. 3, pp. 697-723, 2021. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/SITITO.17.202103.697-723

[9] R. Carolina, "Law and Regulation Knowledge Area," in: *CyBOK: Cyber Security Body of Knowledge*. Version 1.0. A. Rashid, H. Chivers, G. Danezis, E. Lupu, A. Martin Eds. The National Cyber Security Centre, 2019, pp. 49-144. Available: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf (In Russ., abstract in Eng.)

[10] E. A. Ilyushin, D. E. Namiot, and I. V. Chizhov, "Attacks on Machine Learning Systems – Common Problems and Methods," *International Journal of Open Information Technologies*, vol. 10, no. 3, pp. 17-22, 2022. [Online]. Available: https://elibrary.ru/item.asp?id=48102861 (In Russ., abstract in Eng.)

[11] D. E. Namiot, and V. A. Sukhomlin, "On Cybersecurity of the Internet of Things Systems," *International Journal of Open Information Technologies*, vol. 11, no. 2, pp. 85-97, 2023. [Online]. Available: https://www.elibrary.ru/item.asp?id=50271028 (In Russ., abstract in Eng.)

[12] S. V. Lebed, "Innovative Technologies in Cybersecurity," *Modern Information Technologies and IT-Education*, vol. 18, no. 2, pp. 383-390, 2022. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/SITITO.18.202202.383-390

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, (e-mail: sukhomlin@mail.ru).