

УДК 004.056

Г.П. ГАВДАН, В.Г. ИВАНЕНКО

Национальный исследовательский ядерный университет «МИФИ», Москва

К ВОПРОСУ О ПОДГОТОВКЕ ВЫСШЕЙ ШКОЛОЙ КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Рассматриваются вопросы подготовки кадров по информационной безопасности в аспекте обеспечения технологической независимости критической инфраструктуры, не утратившие сегодня своей актуальности. Приоритетным направлением в Море (в том числе и России) остаётся совершенствование Программы высшего образования и качественной подготовки выпускаемых кадров. Предметом исследования (в условиях существования различных угроз безопасности информации является Высшая школа. Проведённый анализ научных публикаций и др. источников по теме исследования показал, что в данной области имеются проблемы. По результатам работы установлено, что в данной области сегодня ещё имеются нерешенные вопросы.

Введение

Подготовка специалистов по направлению информационная безопасность (ИБ) продолжает оставаться достаточно важной и сложной задачей, которая, тем не менее, сегодня решается. Большинство специализированных кафедр вузов продолжают и реализовывать основные образовательные программы высшего образования, в меньшей степени уделяя внимание программам повышения квалификации (ПК) и профессиональной переподготовки (ПП) по направлению в аспекте обеспечения технологической независимости критической информационной инфраструктуры (ОТНКИИ) [1].

Подготовка Высшей школой кадров в области ИБ

По предварительным расчётам Госкорпорации «Росатом, для достижения и обеспечения технологического суверенитета России к 2027 г. понадобится около 51 тыс. специалистов, задействованных в создании и эксплуатации решений для КИИ, а к 2030 г. – 115 тыс. специалистов [2].

Направленность опубликованного Пентагоном Cyber Workforce Focus (CWF, «Плана реализации стратегии кибертрудовых ресурсов на 2023–2027 гг. годь»), является продолжением Стратегии кибербезопасности США на 2023–2027 гг. [3]. В нём представлены проблемные области, такие как выявление, набор, развитие и удержание. Программой предполагается устранение дефицита за счёт применение государственного и частного партнерства, и принятия

дополнительных специальных мер [4]. Обучение талантов и их поиск, необходимо начинать в детских садах и школах. Подростков и детей увлекать ИТ-технологиями, инженерией, математикой и кибернетикой [4]. Применение в Российской Федерации таких же мер явно бы способствовало ликвидации своего дефицита рабочей силы, что является важной задачей.

Развитие кадрового потенциала в области обеспечения ИБ в аспекте ОТНКИИ и применения информационных технологий (ИТ) может решаться самостоятельно, путем обучения персонала, дискуссий, тренингов, дебатов и др. в соответствии с Политикой подготовки персонала в сфере ИБ [5] в аспекте ОТНКИИ; реализацией Программ в вузах обязательно опираясь на опыт зарубежных коллег [6].

Заключение

Решение проблемы дефицита «кибербезопасников» в России (подготовки, ускорения найма и их удержания: военных, гражданских и служащих) что требует (также как и в США) разработки и принятия, специальных мер. Такое развитие кадрового потенциала по направлению информационная безопасность в аспекте ОТНКИИ должно в настоящее время решаться в России как можно быстрее и качественнее.

Список литературы

1. Гавдан, Г.П. Подготовка для Высшей школы кадров по информационной безопасности / Г.П. Гавдан, В. Г. Иваненко // Кибернетика и информационная безопасность «КИБ-2023»: Сборник научных трудов Всероссийской научно-технической конференции, Москва, 18–19 октября 2023 года. – М.: НИЯУ МИФИ, 2023. – С. 154–155. – EDN CSSFXG (дата обращения: 09.09.2024).
2. Е. Абакумов (выступление). Трек обзорно-дискуссионных заседаний «Доверенные РЭУ и ЭКБ для критической гражданской инфраструктуры». // Материалы 9-я научная конференция «ЭКБ и микроэлектронные модули», Форума «Микроэлектроника 2023» <https://microelectronica.pro/albomyi-provedeniya-foruma-2023> (дата обращения: 11.10.2023).
3. Мельников, Д.А. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности / Д.А. Мельников, Г.П. Гавдан, И.А. Корсаков // Безопасность информационных технологий. – 2018. – Т. 25, № 2. – С. 23–37. – EDN XRDUYBF, doi: <http://dx.doi.org/10.26583/bit.2018.2.02> (дата обращения: 09.09.2024)..
4. Горбатов, Виктор С.; Дураковский, Анатолий П. и др. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.I.], v. 26, p. 4, p. 54–68, дек. 2019. ISSN 2074-7136. Доступно на: <https://bit.spels.ru/index.php/bit/article/view/1231>. (дата обращения: 09.09.2024). doi:<http://dx.doi.org/10.26583/bit.2019.4.04>.
5. «DoD Cyber Workforce Strategy Implementation Plan 2023-2027» CLEARED For Open Publication (Jul 13, 2023) Department of Defense. OFFICE OF PREPUBLICATION AND SECURITY REVIEW. URL: <https://dodcio.defense.gov/Portals/0/Documents/Library/CW-StrategyImplementationPlan.pdf> (дата обращения: 19.09.2023).
6. «США не хватает сотен тысяч специалистов в области кибербеза». Эшелон в телеграм канале. URL: <https://t.me/EchelonEyes/1834> (дата обращения: 19.09.2023).