

ФОРМИРОВАНИЕ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В.В. Золотов

*Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Аннотация. В статье рассматриваются актуальные вопросы подготовки специалистов в области защиты информации. Анализируется разрыв между фундаментальными знаниями, изложенными в классических трудах (В.Ф. Шаньгин), и современными требованиями к практическим навыкам выпускников. На основе исследований последних лет (Д.П. Зегжда, С.С. Корт) обосновывается необходимость внедрения в учебный процесс активных методов обучения, включая моделирование угроз и решение практических задач. Предложены пути интеграции фундаментальной подготовки и практико-ориентированного обучения

Ключевые слова: информационная безопасность; подготовка кадров; профессиональные компетенции; высшее образование; киберугрозы; учебный план; моделирование угроз; практико-ориентированное обучение; формирование навыков; киберполигоны.

FORMATION OF PROFESSIONAL COMPETENCIES OF INFORMATION SECURITY SPECIALISTS

V.V. Zolotov

*Educational Institution “Belarusian State University of Informatics
and Radioelectronics”, Minsk, Republic of Belarus*

Abstract. The article deals with topical issues of training specialists in the field of information security. The gap between the fundamental knowledge presented in classical works (V.F. Shangin) and modern requirements for graduates' practical skills is analyzed. Based on recent research (D.P. Zegzhda, S.S. Kort), the necessity of introducing active learning methods, including threat modeling and solving practical problems, into the educational process is substantiated. Ways to integrate fundamental training and practice-oriented learning are proposed.

Keywords: information security; personnel training; professional competencies; higher education; cyber threats; curriculum; threat modeling; practice-oriented learning; skills formation; cyber ranges.

Введение

Современный этап развития информационного общества характеризуется стремительным ростом количества и сложности киберугроз. В этих условиях качество подготовки специалистов по защите

информации становится критическим фактором обеспечения национальной безопасности любого государства. Однако система высшего образования сталкивается с серьезным вызовом: с одной стороны, необходимо дать студентам фундаментальные знания, без которых невозможно понимание основ информационной безопасности, с другой – подготовить выпускника, способного сразу после окончания вуза решать реальные практические задачи. Целью данной работы является анализ существующих подходов к подготовке кадров в области защиты информации и определение путей совершенствования образовательных программ на основе интеграции фундаментальных знаний и современных практико-ориентированных методик.

Основная часть

Фундаментальной основой подготовки специалистов по защите информации являются классические труды, среди которых особое место занимает учебник В.Ф. Шаньгина «Информационная безопасность и защита информации». В нем изложены базовые принципы комплексной системы защиты информации, включая обеспечение конфиденциальности, целостности и доступности данных, а также архитектура защищенных систем и организационно-правовые аспекты. Однако, как показывают исследования последних лет, одного фундаментального образования недостаточно. В работе Д.П. Зегжды с соавторами доказывается, что наибольшую эффективность демонстрирует обучение, построенное на активном вовлечении студентов в решение практических задач, в частности через моделирование угроз, когда студенты самостоятельно строят модели нарушителя и разрабатывают меры противодействия.

С.С. Корт развивает эту мысль, указывая на необходимость создания в вузах киберполигонов – программно-аппаратных комплексов, имитирующих реальную информационную инфраструктуру, где студенты отрабатывают навыки обнаружения и отражения атак. Такой подход формирует профессиональные компетенции – способность применять знания в реальных ситуациях. Еще одним важным аспектом является обучение управлению информационными рисками. Как отмечает А.М. Астахов, специалист должен понимать не только техническую, но и экономическую сторону: обосновывать необходимость средств защиты и оценивать эффективность инвестиций в безопасность. Таким образом, оптимальная модель подготовки специалиста представляет собой синтез трех компонентов: фундаментальной теоретической подготовки (Шаньгин В.Ф.), практической отработки навыков на киберполигонах и в ходе моделирования угроз (Зегжда Д.П., Корт С.С.), а также изучения вопросов управления рисками и экономики безопасности (Астахов А.М.).

Information about the authors

Проведенный анализ позволяет сделать вывод о необходимости модернизации образовательных программ по направлению «Информационная безопасность». Классическая фундаментальная подготовка, представленная трудами В.Ф. Шаньгина, остается необходимой основой, однако она должна быть дополнена современными практико-ориентированными методиками, описанными в работах Зегжды Д.П., Корта С.С. и Астахова А.М. Только сочетание глубоких теоретических знаний и устойчивых практических навыков, сформированных в процессе активного обучения, позволит готовить специалистов, способных эффективно противостоять современным киберугрозам. Перспективным направлением дальнейших исследований является разработка конкретных методик интеграции киберполигонов в учебный процесс и создание системы оценки сформированности профессиональных компетенций.

Список использованных источников

1. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – 3-е изд., перераб.
2. Зегжда, Д.П. Подход к формированию профессиональных компетенций в области информационной безопасности на основе активных методов обучения / Д.П. Зегжда, А.Н. Ковтун, Е.Ю. Павленко // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 45-54.
3. Астахов, А.М. Искусство управления информационными рисками / А.М. Астахов. – М.: ДМК Пресс, 2022. – 320 с.
4. Корт, С.С. Теоретические основы подготовки специалистов по защите информации в условиях цифровой трансформации / С.С. Корт // Безопасность информационных технологий. – 2024. – Т. 31, № 1. – С. 92-103

References

1. Shangin, V.F. Information Security and Information Protection / V.F. Shangin. – 3rd ed., revised and updated. – Moscow: DMK Press, 2020. – 702 p.
2. Zegzhda, D.P. Approach to the Formation of Professional Competencies in the Field of Information Security Based on Active Learning Methods / D.P. Zegzhda, A.N. Kovtun, E.Y. Pavlenko // Cybersecurity Issues. – 2023. – No. 4(56). – P. 45-54.
3. Astakhov, A.M. The Art of Information Risk Management / A.M. Astakhov. – Moscow: DMK Press, 2022. – 320 p.
4. Kort, S.S. Theoretical Foundations of Training Information Security Specialists in the Context of Digital Transformation / S.S. Kort // Information Technology Security. – 2024. – Vol. 31, No. 1. – P. 92-103.

Сведения об авторе

Золотов В.В., курсант учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», e-mail: vadimzolotov94@gmail.com.

Information about the author

Zolotov V.V., cadet of Educational Institution “Belarusian State University of Informatics and Radioelectronics”, e-mail: vadimzolotov94@gmail.com.