этот игровой движок особенно популярен среди инди-разработчиков, что связано с его интуитивно понятным интерфейсом и приятной ценовой политикой компании.

Таким образом, разработка компьютерной игры жанра «визуальная новелла» требует написания качественного интересного сценария, дополнения его иллюстрациями с красочными изображениями, подбора соответствующего музыкального и звукового сопровождения, а также разработки достаточно большего количества сюжетных ветвлений. При этом важно помнить, что, хотя родиной визуальных новелл является Япония, но совершенно не обязательно разрабатывать игры в японском стиле, главное тщательно продумать сюжет, подобрать, а лучше самостоятельно нарисовать изображения, а для реализации игры использовать качественные, популярные и простые в освоении игровые движки.

Список литературы

1. *AJA* Anime Industry Report 2020. URL: https://aja.gr.jp/english/japan-anime-data (дата обращения: 16.03.2022).

2. *Google* for Games Beyond 2021: Where does gaming go next?. URL: https://games.withgoogle.com/reports/#section_blue-island (дата обращения: 16.03.2022).

3. *Stopgame.ru* Визуальные новеллы, что это и с чем едят?. URL: http://bit.ly/2qdSvfj (дата обращения: 16.03.2022).

4. *Saikono* Joker. URL: https://tiny-bunny.fandom.com/ru/wiki/Saikono_Joker (дата обращения: 16.03.2022).

5. *Soviet* Games: Visual Novel Studio. URL: https://sovietgames.su (дата обращения: 16.03.2022).

УДК 378:004.056

А. Д. Третьяков, Н. В. Третьякова
A. D. Tretyakov, N. V. Tretyakova
ФГАОУ ВО «Российский государственный профессионально-педагогический университет», Екатеринбург
Russian state vocational pedagogical university, Ekaterinburg
tretjakovnat@mail.ru

К ВОПРОСУ О ПОДГОТОВКЕ ИТ-СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ON THE ISSUE OF TRAINING IT-SPECIALISTS IN THE FIELD OF INFORMATION SECURITY

Аннотация. Обеспечение информационной безопасности экономики ставит на повестку вопросы об управлении рисками информационной безопасности и предъявляет повышенные требования к уровню профессионализма ИТ-специалистов. В статье дан обзор данных требований и показаны подходы к обеспечению качества образования данных специалистов: своевременное и систематическое выявление недостающих навыков, необходимых ИТ-специалистам для обеспечения информационной безопасности; своевременное обновление содержания образовательных программ; преимущественное использование практико-ориентированных методик обучения на площадках производственных организаций под сопровождением наставника от организации.

Abstract. Ensuring the information security of the economy puts on the agenda the issues of information security risk management and imposes increased requirements on the level of professional competence of IT specialists. The article provides an overview of these requirements and shows approaches to ensuring the quality of education of these specialists: timely and systematic identification of missing skills necessary for IT specialists to ensure information security; timely updating of the content of educational programs; the predominant use of practice-oriented training methods at the sites of production organizations under the support of a mentor from the organization.

Ключевые слова: информационная безопасность, уровень профессионализма ИТ-специалистов, навыки ИТ-специалистов по информационной безопасности, обновление содержание образовательных программ и методик подготовки.

Keywords: information security, the level of professionalism of IT specialists, the skills of IT specialists in information security, updating the content of educational programs and training methods.

Стремительное развитие цифровых технологий обеспечило переход всех стран мира на цифровую экономику. Во всех ее секторах и практически на всех уровнях управления наблюдается стремительные процессы цифровизации, что в свою очередь требует обеспечения соответствующего уровня безопасности оперируемой информацией. Сегодня можно наблюдать значительное число массовых взломов информационных систем как отраслевых организаций любого уровня, так и организаций аппарата государственного управления [2, 3].

Еще недавно обеспечение информационной безопасности считалось проблемой информационно-компьютерных технологий – ИКТ, и к рискам производства не относилась. Сегодня информационная безопасность стала существенной частью управления, ее задачами стали процесс минимизации риска для информационного пространства организации и предотвращение любых инцидентов информационных атак и опасностей. Информационная безопасность сегодня – признанный бизнес-риск. Она проявляется в организационных, человеческих и социальных аспектах бизнес-процессов. В данной связи поднимается задача долгосрочных изменений в подходе к тому, как и кому следует управлять рисками информационной безопасности.

Необходимость обновлять знания, навыки и потенциал в области информационной безопасности привела к созданию ряда стратегических инициатив правительства Российской Федерации и, прежде всего, федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изменениями и дополнениями, вступившими в силу от 01.01.2022); федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (редакция от 02.07.2021); федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (редакция от 09.03.2021). Образовательная часть этих стратегий чаще всего формулируется как стратегии улучшения общего состояния информационной безопасности, куда входит и образование.

Важность знаний об информационной безопасности в настоящее время широко признана, но необходимость их широкого применения зависит от уровня профессионализма специалистов организаций, прежде всего, ИТ-специалистов [4]. Следует отметить, что навыки, необходимые ИТ-специалистам для обеспечения информационной безопасности стремительно меняются, вследствие быстрых темпов развития цифровых технологий и быстрой цифровизации общества. Исследование ИКТ-навыков, ежегодно проводимое Enterprise Strategy Group – ESG, показало, что разрыв в навыках в области информационной безопасности увеличивается и за последние пять лет удвоился **[6**]. Быстрая эволюция информационных атак и опасностей в сочетании со статичным характером академического образования, характерного для высших учебных заведений, способствовала появлению несоответствий между знаниями, преподаваемыми в рамках образовательных программ, и навыками, ожидаемыми работодателями, тем самым способствуя увеличению разрыва в навыках ИТ-специалистов по информационной безопасности. Соответственно, образование в области информационной безопасности нуждается в обновлении для применения в системе образования, на уровне содержания и технологий обучения специальности, и в соответствующей отрасли, на уровне развития и совершенствование ранее сформированных профессиональных компетенций через дополнительное профессиональное образование, внутрифирменное обучение и др.

Сегодня высшие учебные заведения работают над решением проблемы растущей нехватки навыков в области информационной безопасности. Однако анализ образовательных программ как отечественных, так и зарубежных высших учебных заведений, показывает, что содержание наполнено традиционными разделами и темами по информационной безопасности (основные компьютерные архитектуры, данные, криптография, сети, принципы безопасного кодирования и внутреннего устройства операционной системы и др.), а применению инновационных практико-ориентированных методик обуче-

ния и использованию, так называемых, полигонных платформ уделяется явно недостаточное внимание [1, 5].

Между тем, своевременное и систематическое выявление недостающих навыков, необходимых ИТ-специалистам для обеспечения информационной безопасности, позволяет своевременно обновлять как содержание образовательных программ, так и методики обучения. Так, например, по данным исследования **ESG [6**] в числе самых основных недостатков навыков информационной безопасности в технологической области являются «Безопасность облачных вычислений» (39%), «Анализ безопасности и исследования» и «Безопасность приложений» (30%), «Управление рисками и/или соблюдением требований» (27%), «Инженерия безопасности» (22%), «Тестирование на проникновение» (18%), «Аудиты безопасности» (16%), «Сетевая безопасность» (12%), «Безопасность мобильных компьютеров» (8%). «Безопасность базы данных» (6%) и др. Соотношение данных ESG с запросами работодателей и требованиями федеральных образовательных стандартов позволят своевременно обновлять учебные планы, тематику разделов и тем учебных дисциплин в подготовке ИТ-специалистов. Основанием для корректировки применяемых методик обучения также могут служить полученные данные той же ESG. В частности, установлено, что для карьеры специалиста по информационной безопасности наиболее важным является наличие практического опыта (52%), с преимущественным получением опыта в отраслевой организации (42%) и непосредственным сопровождением наставника (36%) [6**]**. Соответственно, подготовка должна быть преимущественно практико-ориентированной, в тесной связи и на площадках конкретных производственных организаций, а также предусматривать наличие сопровождения наставником от организации.

Таким образом, обеспечение качества подготовки и, соответственно, востребованность ИТ-специалистов по информационной безопасности предполагает систематическое отслеживание требований, предъявляемых к уровню профессионализма данных специалистов в мировой экономике и на основании полученных данных своевременное обновление содержания образовательных программ и обеспечение их практико-ориентированности.

Список литературы

1. *Лавина Т. А., Ильина Л. А.* Подготовка по информатике будущих специалистов по защите информации: содержательный аспект // Вестник Череповецкого государственного университета. 2020. № 1 (94). С. 173–184. https://doi.org/10.23859/1994-0637-2020-1-94-15**.**
2. *Тагирова Д. Р.* Кибератака и большие данные как современный вид угроз энергобезопасности // Вестник магистратуры. 2021. № 7 (118). С. 34–36.
3. *Borka J. B.* The cybersecurity labour shortage in Europe: Moving to a new concept for education and training // Technology in Society. 2021. Vol. 67. P. 101769. https://doi.org/10.1016/j.techsoc.2021.101769.
4. *Caulkins B., Marlowe T., Reardon A.* Cybersecurity Skills to Address Today's Threats // Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing. 2019. Vol. 782. P. 187–192. https://doi.org/10.1007/978-3-319-94782-2_18.
5. *Gaps* in European Cyber Education and Professional Training. URL: https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.
6. *Oltisk J.* Enterprise strategy group // ESG Infographic: the Life and Times of Cybersecurity Professionals 2021Cybersecurity Pending Trends. URL: https://www.esg-global.com/research/esg-infographic-the-life-and-times-of-cybersecurity-professionals-2021.