Методы и средства формирования и оценки компетенций специалистов в области информационной безопасности на основе многофункционального программно-аппаратного комплекса

А.В. Шестаков[1], И.Ю. Коцюба[2]

[1] *Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург*
[2] *Университет ИТМО, Санкт-Петербург*

Аннотация. В статье обсуждаются различные аспекты организации обучения специалистов в области информационной безопасности на основе киберполигона – многофункционального программно-аппаратного комплекса. Приводится анализ сущности киберполигона как компьютерной технологии обучения в рамках процессов цифровизации образования и формирования компетенций обучающихся, например, цифровой культуры и кибергигиены. На основе анализа возможностей киберполигона для подготовки и переподготовки специалистов различных профилей сформулированы требования к специфике методов и средств обучения и оценки их компетенций. Обсуждаются проблемы концептуального проектирования образовательного контента киберполигона, необходимость формализованного описания сущностей компетенций и их составляющих, фиксации причинно-следственных связей для сценарного проектирования образовательных траекторий. Отдельное внимание уделено специфике педагогического проектирования, использованию активных и групповых подходов к обучению, необходимости распределения ролей при решении командных задач. Предложены новые формальные подходы к концептуальному проектированию сущностей компетенций с учетом данной специфики, методы автоматизированного распределения участников по ролям учебных проектов и учебным задачам, новые концептуальные модели оценки компетенций на основе покрытия их подходящими компетентностно-ориентированными заданиями. Предложенные концептуальные модели легли в основу программной архитектуры информационных компонент киберполигона по управлению образовательными траекториями и представлены на уровне артефактов проектирования логического уровня системы управления киберполигоном.

Ключевые слова: киберполигон, информационная безопасность, кибергигиена, цифровизация образования, цифровая культура, концептуальное проектирование, методы автоматизированного распределения, модели оценки компетенций, артефакты проектирования.

Введение

Современное образование нацелено на активное использование информационных технологий, которые могут рассматриваться, как средства управления логикой образовательных траекторий, поддержки образовательного процесса, в том числе, через предоставление удобной инфраструктуры тренажерного характера, взаимодействия субъектов

образовательного процесса в едином пространстве, и т.д.

Киберполигон [1,2] представляет собой инфраструктуру для оттачивания умений и практических навыков обучаемых (специалистов, должностных лиц) для взаимодействия с экспертами различных направлений, руководителей специальных подразделений и организаций в сфере информационных технологий и информационной безопасности, а также для испытаний программного и аппаратного обеспечения через имитацию компьютерных атак и отработку реакций на них, что позволяет, например, обнаруживать уязвимости в IT-инфраструктуре без проведения деформационных и трудозатратных тестов на собственных ресурсах.

Уровень существующих технологий и требования к обеспечению адекватности (подобию) исследуемых процессов и инфраструктур позволяют реализовать киберполигоны с компонентами действующей информационной инфраструктуры, формируя киберфизические системы.

Киберфизические системы играют центральную роль в новой цифровой экономике, поскольку они служат связующим звеном между физическим и виртуальным миром, повышают эффективность функционирования объектов реальных секторов экономики, на основе обработки и хранения больших массивов данных, применения сервисов облачных технологий. Развитие цифрового пространства обусловливает активное внедрение таких систем и технологий и в киберполигон.

В ходе кибертренировок и киберучений выявляются ошибки участников, которые после анализа и разбора позволят получить ценный опыт без ущерба для безопасности реальной информационной инфраструктуры. Учебные тренировки максимально приближены к реальным условиям, поэтому многократная отработка проблемных ситуаций приведет к новым профессиональным навыкам и умениям, что в последующем приведет к более эффективным действиям на реальных объектах информатизации,

информационной инфраструктуре.

Создание лабораторного комплекса киберполигона дает возможность совершенствовать не только навыки практической отработки противодействия компьютерным атакам, но и знания, и умения, что позволяет взглянуть на перспективы использования киберполигона в широком, компетентностно-ориентированном подходе к обучению.

Ряд проблемных аспектов связан с развертыванием инфраструктуры киберполигона и сопровождением программных и аппаратно-программных средств комплекса. Этот аспект достаточно проработан и определен регламентирующими документами, например, ГОСТ Р ИСО/МЭК 15408-1, 15408-2, 15408-3; ISO/IEC 18045, и должен рассматриваться как "управление конфигурацией" (деятельность по мониторингу, контролю и руководству документированием характеристик компонент киберполигона) на всем периоде жизненного цикла киберполигона (как представлено на рисунке 1). Следовательно, необходимо осуществлять комплексное управление жизненным циклом информационной системы киберполигона с момента анализа предметной области до этапа внедрения и сопровождения, а учет спектра требований к ней порождает проблему учета педагогической специфики полноты всего комплекса задач по обучению специалистов в период эксплуатации киберполигона.

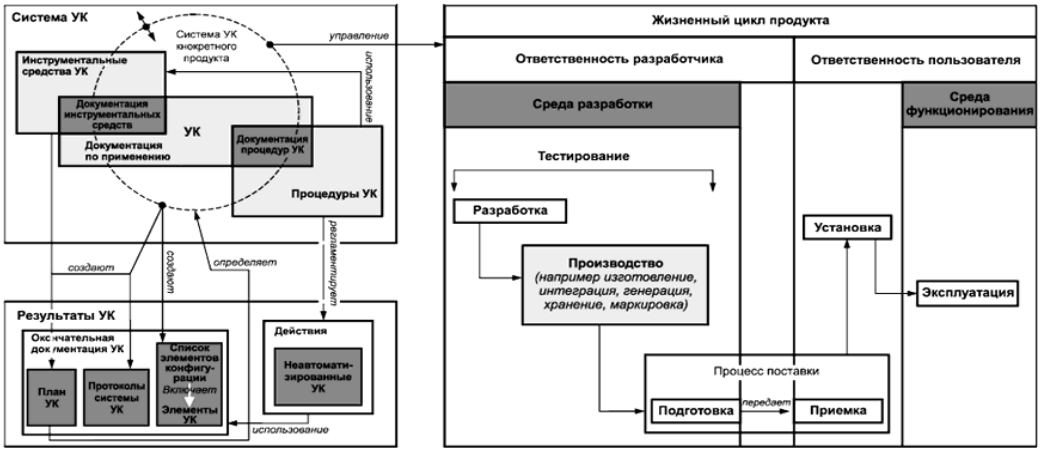

Рисунок 1. - Взаимосвязь системы управления конфигурацией киберполигона

Решение вопроса кибербезопасности информационных систем подчеркивает важность задачи практической оценки эффективности инструментов киберзащиты. Эта задача может быть решена через воссоздание условий информационного взаимодействия, что обеспечивает достаточное сходство с реальными условиями работы систем защиты и атакующих инструментов с точки зрения рассматриваемых процессов и явлений, а также анализ возможных сценариев развития ситуаций. Моделирование включает формализацию логической последовательности: взаимодействие множества обнаруженных уязвимостей ПО, актуальных угроз, вероятных сценариев реализации угроз и возможных киберфизических последствий с количественной оценкой рисков нарушения кибербезопасности. Основная цель моделирования при организации киберучений (кибертренировок) — поиск оптимальных решений для системного реагирования на целенаправленные атаки, а также оценка эффективности принятых решений для нейтрализации киберугроз и изучение влияния различных угроз на сложную взаимозависимую информационную инфраструктуру.

В вопросах обучения специалистов информационной безопасности также необходимо учитывать отраслевую специфику. Например, в Военном университете радиоэлектроники (ВУРЭ), где основное внимание уделяется техническому обучению, студенты должны освоить навыки установки, настройки и разработки программного обеспечения через практические занятия и лабораторные работы. Для этих целей может применяться киберполигон. Комплексность разработки и применения киберполигона требует учета таких специфических особенностей, как:

- концептуальное проектирование составных сущностей формируемых компетенций обучающихся;

- проектирование средств формирования и оценки компетенций

специалистов в области информационной безопасности;

- формирование сценариев причинно-следственных взаимосвязей между формируемыми компетенциями;

- использование особых педагогических методов и средств (например, активных методов обучения);

- управление решением командных задач, в том числе распределением исполнителей по ролям внутри команды;

- учет специфики отраслевой принадлежности обучающихся информационной безопасности (например, в военной сфере, силовых ведомствах и т.д.)

Управление разработкой киберполигона на уровне концептуального компетентностного проектирования

Как показал анализ публикаций по проблематике киберполигонов [3,4], важно повысить компетентность и осведомленность разработчиков киберполигонов в области безопасного программирования через обучение и тренинги, включая в том числе игровые, групповые форматы. Применение групповых методов обучения имеет ряд преимуществ [5,6]:

- возможность учащимся активно участвовать в учебном и воспитательном процессе: устанавливать цели, планировать их выполнение, самостоятельно изучать новые темы, оценивать себя и своих товарищей, а также оценивать результаты своей и чужой работы;

- подготавливает к работе в условиях постоянно меняющейся социальной обстановки;

- максимально стимулирует развитие индивидуальных способностей и различных навыков каждого обучающегося: коммуникативные, познавательные навыки;

- различные формы обучения дают возможность обучающихся пробовать себя в новых ролях: как учителя, консультанта, участника

групповой работы, готовя их к самоуправлению.

Один из ключевых моментов эффективной организации группового взаимодействия — тщательное формирование групп [7,8]. Как показал обзор литературы по проблематике обучения специалистов в области информационной безопасности [9-11], существуют различные подходы к классификации и упорядочиванию их компетенций:

а) по уровню квалификации: специалисты высшего, среднего уровня:

- по причинно-следственным классам формируемых компетенций: базовые – отраслевые – профессиональные;

- по корреляции индикаторов знаний в области информационной безопасности;

- по степени выраженности компетенции;

- по уровню сформированности компетенции: на начальном, ознакомительном, профессиональном уровне.

Существуют различные подходы к классификации вариантов представления компетенций специалистов в области информационной безопасности. Задача направлена на описание компетентностной модели индивидуального специалиста, а не дает ответ на вопрос о распределении командных видов работ внутри коллектива сотрудников.

Для формализации описания компетенции специалиста в области информационной безопасности воспользуемся моделью содержательной компетенции:

«деятельность» + «объект деятельности» + «метод, способ формирования».

Составляющую **«объект деятельности»** определим, как список вариантов объектов, на которые направлена программная реализация с использованием киберполигона или обучения информационной безопасности на его основе в соответствии с результатами анализа литературы:

- правила установления инфраструктуры информационной безопасности;

- риски и системные неисправности;

- настройки, программные и физические исправления устанавливаемых компонентов;

- угрозы и уязвимости, характерные для цифровых продуктов;

- режимы и протоколы работы системы.

Составляющую **«метод, способ формирования»** определим, как список вариантов трендовых технологий в области программной реализации киберполигона или обучения информационной безопасности на его основе в соответствии с результатами анализа доступных источников:

- на основе облачных центров;

- посредством сертифицированных продуктов и сервисов для поддержки создания облачных приложений;

- с использованием облачных, туманных, квантовых технологий;

- в системах виртуальной и дополненной реальности;

- на основе систем искусственного интеллекта;

- с использованием сигнатурных, поведенческих, комбинированных методов;

- посредством тренингов, в игровом формате.

Предложенный формат лингвистического описания составных сущностей компетенций, а также способов их классификации в соответствии с (1) позволил перейти к их программному представлению на уровне моделей концептуального проектирования (рисунок 2).

Каждому из классов присвоены свои методы, через которые происходит взаимодействие с классом «Course». Класс «Course», в свою очередь, определяется классом «Module» и связан композиционным отношением, что подчеркивает зависимость класса «Module» от класса «Course». «Module» в

свою очередь состоит из классов «Lecture» и «Test».

Класс «Task» объединяется агрегированным отношением с классом «Lecture», что подчеркивает не полную зависимость заданий от лекций, т.е. родительский класс может существовать без дочернего класса.

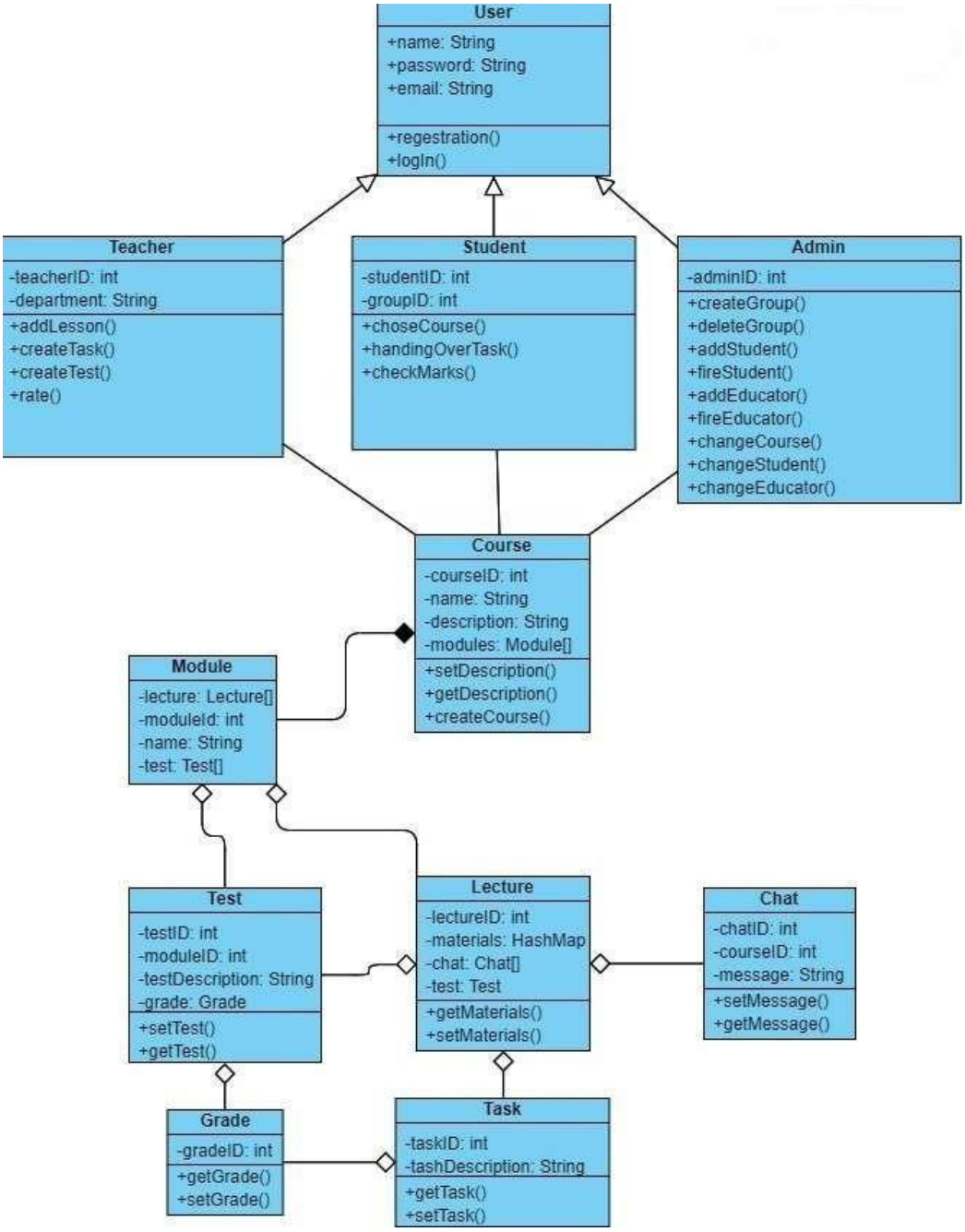

Рисунок 2. – Модель концептуального описания компетенций для управления групповой работой специалистов в области информационной безопасности

Класс «Grade» также связан агрегированным отношением с классами

«Test» и «Task», как и класс «Chat» связна с классом «Lecture».

Класс «**Grade**» используется для формализованного описания уровня сформированности компетенции специалиста (в соответствии с (1)).

Класс «**Task**» позволяет формализовать описание различных компетентностно-ориентированных заданий для оценки сформированности компетенций. Стоит отметить, что важным атрибутом класса «**Task**» является его нечеткая принадлежность, которая позволяет описать «степень принадлежности» задания к оценке формируемой компетенции. Ввиду командной работы специалистов этот атрибут позволит значительно сократить количество компетентностно-ориентированных заданий, поскольку будет отсутствовать строгое структурное разделение заданий по отдельным компетенциям или специалистам и правило аддитивности, а одно и то же задание со степенью нечеткой оценки сможет быть ассоциировано с большим количеством измеряемых компетенций и охватить сразу нескольких специалистов.

Значения, хранящиеся в классе «**Grade**», могут быть ассоциированы с критерием оптимизации «полезность» в целевой функции. Для решения подобного класса задач могут использоваться методы комбинаторной оптимизации, а содержательная интерпретация полученных значений производиться с учетом постановки задачи со сформулированными специфическими особенностями управления компетенциями обучающихся (специалистов) в области информационной безопасности.

Заключение

Предложенные методы позволят значительно поддержать процесс концептуального проектирования киберполигона, осуществить сценарное описание причинно-следственных мероприятий по обучению специалистов в области информационной безопасности. На основе формализации множеств обучающих мероприятий могут быть сгенерированы вариативные кейсы для

обучения специалистов с учетом специфики командной работы, а также можно формализовать процесс управления комплектациями команд.

Статья подготовлена в рамках выполнения в 2023 году прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР № 123030100009-7 от 01.03.2023.

Литература

1. Горячев С. Н., Михалев В. В., Кобяков Н. С., Русских В. Н. Опыт создания макета критической инфраструктуры организации // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2023. №1 (60). С. 63-69.
2. Назарова О.Г., Клименко А.Д. Информационная безопасность в период становления цифровой экономики В России // Экономика. Социология. Право. 2020. №2 (18). С. 35-41.
3. Пакляченко М. Ю. Безопасность цифровых продуктов и услуг: принципы и элементы безопасного дизайна // Вестник Московского университета МВД России. 2023. №1. С. 308-314.
4. Ульянов А. Н., Столяров М. Г., Стельмах И. В. Применение технологий виртуализации вычислительных ресурсов в информационно-образовательной среде // ВВО. 2021. №6 (33). С. 66-69.
5. Полякова Т. А., Бойченко И. С. Информационная безопасность через призму национального проекта «Цифровая экономика»: правовые проблемы и векторы решений // Право и государство: теория и практика. 2019. №2 (170). С. 97-100.
6. Метельков А. Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. 2022. №1. С.51-60.

7. Жуков М. М., Баркалов Ю. М., Телков А. Ю. Методологический подход к имитационному моделированию при исследовании практической эффективности систем защиты от сетевых кибератак // Вестник ВИ МВД России. 2022. №1. С. 24-39.

8. Углов А.Е., Клюев С.Г., Петухов А.Ю. Умение и навыки. результаты педагогического эксперимента по использованию вычислительных мощностей ПАК «Киберполигон» для формирования умений и практических навыков администрирования комплекса средств защиты операционной системы специального назначения «ASTRA LINUX» // ВВО. 2023. №4 (43). С. 64-67.

9. Бабкин А.Н., Перминов Г.В. Алгоритм оценки сформированности компетенций специалистов по защите информации // Известия Воронежского государственного педагогического университета, №4(289), 2020 С. 93-100.

10. Комаров В.В. Исследование квалификационных дефицитов руководителей и специалистов, ответственных за вопросы градостроительства на муниципальном уровне (на примере Самарского региона) // Экономика, предпринимательство и право. –2022. – Том 12. – № 2. – С. 897-918.

11. Сладкова Н.М., Ильченко О.А., Степаненко А.А., Шапошников В.А. Особенности оценки компетенций по информационной безопасности государственных и муниципальных служащих // Вопросы государственного и муниципального управления. 2021.№1.– С. 122-149.

References

1. Goryachev S. N., Mihalev V. V., Kobyakov N. S., Russkih V. N. Vestnik Permskogo universiteta. Seriya: Matematika. Mekhanika. Informatika. 2023. №1 (60). pp. 63- 69.

2. Nazarova O.G., Klimenko A.D. Ekonomika. Sociologiya. Pravo. 2020. №2 (18). pp. 35-41.

3. Paklyachenko M. YU. Vestnik Moskovskogo universiteta MVD Rossii. 2023. №1. pp. 308-314.

4. Ul'yanov A. N., Stolyarov M. G., Stel'mah I. V. VVO. 2021. №6 (33). pp. 66-69.

5. Polyakova T. A., Bojchenko I. S. Pravo i gosudarstvo: teoriya i praktika. 2019. №2 (170). pp. 97-100.

6. Metel'kov A. N. Pravovaya informatika. 2022. №1. pp. 51-60.

7. ZHukov M. M., Barkalov YU. M., Telkov A. YUVestnik VI MVD Rossii. 2022. №1. pp. 24-39.

8. Uglov A.E., Klyuev S.G., Petuhov A.YU. VVO. 2023. №4 (43). pp. 64-67.

9. Babkin A.N., Perminov G.V. Izvestiya Voronezhskogo gosudarstvennogo pedagogicheskogo universiteta, №4 (289), 2020, pp. 93-100.

10. Komarov V.V. Ekonomika, predprinimatel'stvo i pravo. 2022. № 2. pp. 897-918.

11. Sladkova N.M., Il'chenko O.A., Stepanenko A.A., Shaposhnikov V.A. Voprosy gosudarstvennogo i municipal'nogo upravleniya. 2021.№1. pp. 122-149.

Дата поступления: 28.10.2023

Дата публикации: 8.12.2023