УДК 371.263

МЕТОДИКА РАЗРАБОТКИ СИСТЕМЫ ТЕСТОВОЙ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Овчинникова И.Г., [2]Чусавитина Г.Н., [2]Курзаева Л.В.

[1]НОУ ВПО «Институт бизнеса, психологии и управления», Химки, e-mail: igo55@mail.ru;
[2]ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», Магнитогорск, e-mail: lkurzaeva@mail.ru

Вопросы подготовки будущих учителей в области информационной безопасности в современном обществе особенно актуальны. Проблеме формирования и оценке сформированности компетенций у студентов вуза в данной области придается важное значение в системе современного высшего образования. Компетентностный подход к обучению позволяет определить требования к содержанию и уровню компетенций в области информационной безопасности на каждой образовательной ступени. В настоящей статье авторы приводят описание методики разработки системы оценки уровня сформированности компетенций бакалавров в области информационной безопасности с использованием рамок квалификаций и таксономии Блума. Раскрываются особенности разработки тестовых заданий различного уровня сложности; приводятся примеры, иллюстрирующие разные типы заданий и их постановку. Представленная статья будет интересна преподавателям, занимающимся вопросами формирования системы оценки сформированности результатов обучения с учетом требований компетентностного подхода.

Ключевые слова: компетентностный подход, средства оценивания результатов обучения

METHOD DEVELOPMENT TEST'S ASSESSMENT SYSTEM OF LEVEL BACHELORS COMPETENCE IN INFORMATION SECURITY

[1]Ovchinnikova I.G., [2]Chusavitina G.N., [2]Kurzaeva L.V.

[1]Institute of Business, Psychology and Management, Khimki, e-mail: igo55@mail.ru;
[2]Nosov Magnitogorsk State Technical University, Magnitogorsk, e-mail: lkurzaeva@mail.ru

Questions of information security in today's society are particularly relevant, and the formation and evaluation of formation of competences in this area is considered important. Competence approach to training allows you to define requirements for the content and level of information security of the individual competencies of each educational stage. In this paper, the authors give description of the method of formation of the development of competences level evaluation system of bachelors in the field of information security with a framework of qualifications and Bloom's taxonomy. The peculiarities of the development of test tasks of different levels of complexity; examples illustrating the different types of jobs and production. The submitted article will be of interest to teachers, dealing with the formation of a system of evaluation of formation of learning outcomes, taking into account the requirements of the competency approach.

Keywords: competence approach, means of assessment of learning outcomes

В современном информационном обществе для обеспечения безопасности информационно-образовательной среды образовательного учреждения, информационной безопасности личности учащегося немаловажную роль играет компетентность учителей по вопросам информационной безопасности и защиты информации.

В ФГОС ВО в разделе VIII установлено требование обязательной оценки уровня знаний и умений обучающихся и уровня приобретённых компетенций, но, к сожалению, текст ФГОС не вносит ясность в вопрос, как оценивать те или иные компетенции. Поэтому на сегодняшний день оценка уровня компетенции представляет большую сложность. Трудность здесь видится в том, что компетенцию нельзя трактовать как сумму предметных знаний и умений. Скорее это усовершенствование существующих и приобретаемые в результате обучения новые способности, увязывающие знания и умения со спектром интегральных характеристик качества подготовки, в том числе и способностью применять полученные знания и умения в решении межпредметных практических задач, в будущей профессиональной деятельности после окончания учебного заведения [2].

Рассмотрим пример построения инструментария оценки компетентности, на примере компетенций в области информационной безопасности.

Для направления подготовки бакалавров «Педагогическое образование», профиль «Информатика», задача может быть представлена междисциплинарным заданием при оценке следующей совокупности компетенций:

– готов использовать основные методы защиты от возможных последствий аварий, катастроф, стихийных бедствий (ОК-11);

– способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12);

– способен формировать и использовать безопасную информационно-образовательную среду (СК-2).

Компетенции являются измеримыми и диагностичными, а значит: во-первых, в основу разработки педагогической составляющей диагностики сформированности результатов обучения должна быть положена таксономия педагогических целей, обеспечивающая учет уровневого характера изменения требований к результатам обучения в системе профессионального образования, например, на основе рамки квалификаций; во-вторых, созданы условия для максимального приближения процедуры оценки к условиям профессиональной деятельности [3].

Последнее соответствует требованию ФГОС ВПО в п. 8.4 «для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ООП (текущая и промежуточная аттестация) создаются фонды оценочных средств, включающие типовые задания, контрольные работы, тесты, позволяющие оценить знания, умения и уровень приобретенных компетенций. Фонды оценочных средств разрабатываются и утверждаются вузом.

Вузом должны быть созданы условия для максимального приближения программ текущего контроля успеваемости и промежуточной аттестации обучающихся к условиям их будущей профессиональной деятельности – для чего, кроме преподавателей конкретной дисциплины, в качестве внешних экспертов должны активно привлекаться работодатели, преподаватели, читающие смежные дисциплины, и так далее».

Так как в современной парадигме кадрового менеджмента при приеме на работу оценка компетенций зачастую производится в рамках Assessment center, то в вузе целесообразно применять аналогичную процедуру. Учитывая это, дальнейшее рассмотрение будет осуществлено в русле комплексной разработки инновационных педагогических средств оценки результатов обучения и подбора и адаптации психологических методик и техник.

Рассмотрим особенности разработки педагогических средств оценки результатов обучения в рамках тестирования.

Приведенное в [3] уровневое описание когнитивной составляющей компетентности в области информационной безопасности может служить основой для проектирования тестовых заданий. Согласно рекомендациям [3], заложенная в основу оценки таксономия Б. Блума может помочь в определении уровня сложности вопросов тестов.

Приведем примеры тестовых заданий по уровням сложности в соответствии с [1; 3].

Первый уровень (знание) – тесты по узнаванию, т.е. отождествлению объекта и его обозначения: задания на опознание, различение или классификацию объектов, явлений и понятий.

Пример 1.

Согласно «Доктрине информационной безопасности РФ», общие методы обеспечения информационной безопасности Российской Федерации разделяются на:

1) правовые, организационные, программно-технические и экономические;

*2) **правовые, организационно-технические и экономические;***

3) законодательные, административные, организационные и технические;

4) нормативно-правовые, программно-технические, экономические.

Второй уровень (понимание) – тесты-подстановки, в которых намеренно пропущено слово, фраза, формула или другой какой-либо существенный элемент текста, и конструктивные тесты, в которых в отличие от теста-подстановки не содержится никакой помощи учащимся даже в виде намеков и требуется дать определение какому-либо понятию, указать случай действия какой-либо закономерности и т.д.

Пример 2.

Вставьте пропущенные слова.

Защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение _____ доступа и воздействия на _____ информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, _____, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования _____.

Ответ: несанкционированного, защищаемую, уничтожению, носителя информации.

Четвертому уровню (анализа и синтеза) соответствуют задания, содержащие

продуктивную деятельность, в процессе которой необходимо использовать знания-умения. В основу тестов данного уровня могут быть положены нетиповые задачи на применение знаний в реальной практической деятельности. Условия задачи формулируются близкими к тем, которые имели место в реальной жизненной обстановке (см. пример 3).

Пример 3.

Приведите примеры из кино- и видеофильмов, иллюстрирующие использование уязвимых мест и нарушения мер защиты информационной безопасности для несанкционированного проникновения в охраняемые системы. Сформулируйте рекомендации, которые способствовали бы предотвращению инцидента нарушения информационной безопасности для каждого примера.

Тесты пятого уровня – это проблемы, решение которых сводится к выполнению творческой деятельности, результатом которой является получение объективно новой информации. Тестами данного уровня выявляется умение ориентироваться и принимать решения в новых, проблемных ситуациях (см. пример 4)

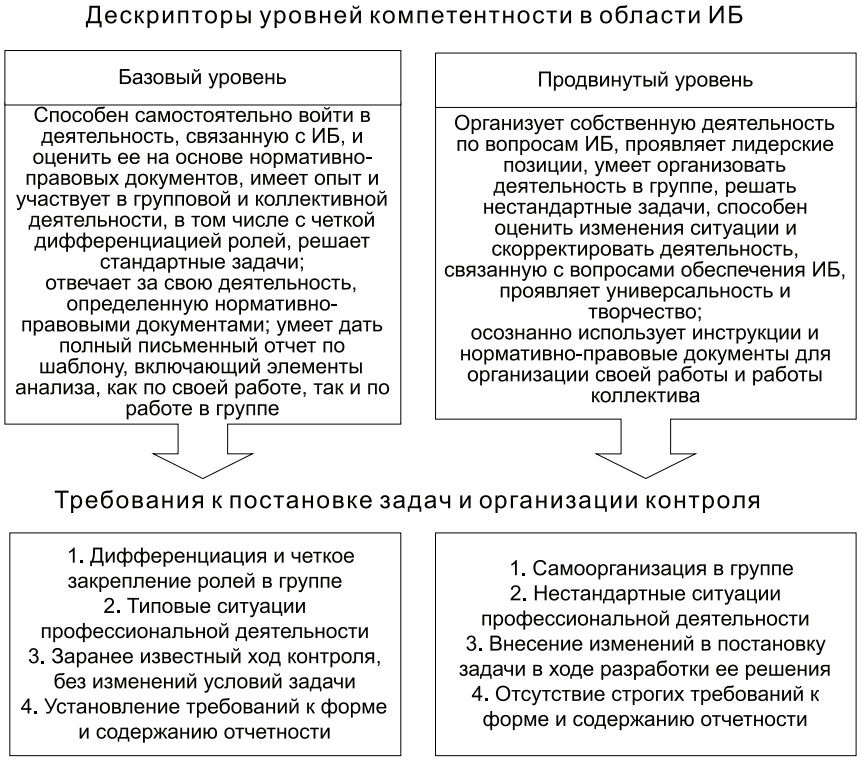
Пример 4.

Проанализируйте состояние информационной безопасности в компьютерном классе вашего учебного заведения. Выполнение идентификацию рисков ИБ.

Указанная выше классификация тестовых заданий позволяет оценить лишь когнитивную составляющую компетентности в области информационной безопасности. В контексте совокупной оценки всех компонентов указанной компетенции особое место занимают *тесты действия и ситуационные тесты.*

Тесты действия (performance tests). Термин взят из психологии, где тесты действия понимаются как *процедура, ориентирующая испытуемого на выполнение какого-нибудь практического действия* (практические испытания). Они позволяют проверить не только уровень овладения навыком, но и оценить различные качества личности и уровень формирования сопутствующих компетенций. Например, могут помочь оценить когнитивный стиль, эстетический вкус, юмор и т.д.

Требования к сложности постановки задач таких тестов можно определить на основе дескрипторов уровней деятельностно-поведенческого компонента компетентности в области информационной безопасности (рисунок).



Постановка задач с учетом требований к уровню сформированности деятельностно-поведенческого компонента компетентности в области информационной безопасности

Приведенный далее пример ориентирован на продвинутый уровень, но при конкретизации задания может быть адаптирован для базового.

Пример 5.

Задание: *Выберите автоматизированную информационную систему, проведите ее анализ в контексте обеспечения организации мер информационной безопасности. Предложите дополнительные мероприятия по повышению уровня информационной безопасности.*

Ситуационные тесты (имитационные методы учебной деятельности) – требуют не произведения реального действия, а его имитации. Одним из популярных видов ситуационных тестов является *анализ конкретной ситуации*. Испытуемым предлагается обширная информация о конкретной ситуации, требуется провести анализ ситуации, при этом испытуемый должен учитывать, что часть информации – лишняя, и у него есть возможность добыть дополнительную информацию (воспользовавшись справочником или задав вопрос). После анализа принимается мотивированное решение.

Пример 6.

Постройте модель возможного нарушителя. Сымитируйте инцидент, связанный с нарушением конфиденциальности персональных данных (ПДн) обусловленный:

– преднамеренными или непреднамеренными действиями лиц, имеющими доступ к информационным ресурсам информационной системы персональных данных (ИСПДн), включая пользователей, реализующие угрозы непосредственно в ИСПДн;

– преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

– угрозами, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;

– со стихийными природными явлениями.

Задание для базового уровня:

Как в рамках определенной политики безопасности служба информационной безопасности будет реагировать на инцидент? Смоделируйте процесс реагирования на инцидент.

Сформируйте отчет об инциденте.

Задание для продвинутого уровня:

Проведите углубленный анализ инцидента, на основе результатов анализа сделайте выводы и подготовьте рекомендации по улучшению процесса обеспечения ИБ и реагирования на инциденты.

Другой, более сложной разновидностью ситуационных тестов является *методика последовательных ситуаций*. Задача разворачивается во времени и решается поэтапно; переход к следующему этапу возможен только в случае правильного ответа на вопросы предыдущего этапа, условия следующего этапа определяются в зависимости от варианта ответа на предыдущем этапе.

Пример 7.

Задание:

1. Проведите аудит информационной безопасности образовательного учреждения, включая:

– постановку задачи и определение объекта аудита.

● *определение задач, целей и объектов аудита информационной безопасности;*

● *формирование рабочей группы (включая специалистов заказчика);*

● *составление регламента проведения работ;*

● *разработка технического задания (ТЗ) на проведение работ.*

– сбор, подготовку и анализ данных для проведения работ:

● *изучение объекта исследования;*

● *анализ организационно-административных мер обеспечения ИБ;*

● *анализ программно-технических средств обеспечения ИБ;*

● *фиксация текущего состояния и характеристик объекта исследования;*

● *определение соответствия характеристик объекта исследования требованиям политики ИБ;*

● *выявление технических уязвимостей объекта исследования.*

2. Подготовьте аналитический отчет по выполненной работе, включая:

– моделирование процессов нарушения системы безопасности;

– определение угроз нарушения ИБ;

– анализ уязвимостей и оценка рисков;

– определение устойчивости объекта в соответствии с требованиями по обеспечению ИБ;

– разработка организационных мер обеспечения ИБ;

– разработка предложения по развитию программно-технических средств обеспечения ИБ;

– разработка рекомендаций по совершенствованию структуры информационной системы;

– разработка рекомендаций по повышению квалификации штатного персонала.

3. Выработайте рекомендации по политике информационной безопасности образовательного учреждения.

4. Разработайте программу обеспечения информационной безопасности образовательного учреждения.

Приведенная методика оценки уровня сформированности компетентности в области информационной безопасности применима для установления соответствия требуемому уровню результатов не только профессионального обучения, но и нефор-мального и внеформального обучения. Таким образом, она может стать основой как для построения системы мониторинга достижения целей конкретной образовательной программы в вузе, так и для создания банка тестовых заданий центров сертификации квалификаций и аттестации кадров.

Список литературы

1. Богословский В.А.. Караваева Е.В.. Ковтун Е.Н.. Мелехова О.П.. Родионова С.Е.. Тарлыков В.А.. Шехонин А.А. Методические рекомендации по проектированию оценочных средств для реализации многоуровневых образовательных программ ВПО при компетентностном подходе. – М.: Изд-во МГУ, 2007. –70 с.

2. Компетентностный подход. Инновационные методы и технологии обучения: учеб. метод. пособ. / сост. Н.В. Соловова. С.В. Николаева. – Самара: Универс групп, 2009. – 70 с.

3. Курзаева Л.В., Овчинникова И.Г., Слепухина Г.В. Психолого-педагогический инструментарий оценки и диагностики результатов обучения личности по направлениям подготовки в сфере ИТ: метод. рекомендации. – Магнитогорск: МаГУ, 2013. – 40 с.

4. Курзаева Л.В., Овчинникова И.Г. Исследование уровней формирования результатов обучения в системе профессионального образования Челябинской области вуза // Спрос и предложение на рынке труда и рынке образовательных услуг в регионах России: сб. докладов по материалам Девятой Всероссийской научно-практической Интернет-конференции (31 октября – 1 ноября 2012 г.). – Кн. III. – Петрозаводск: ПетрГУ, 2012. – С. 228–237.

5. Курзаева Л.В., Чусавитина Г.Н. Подготовка будущих педагогических кадров к превенции киберэкстремизма среди молодежи: моделирование процесса установления требований к процессу профессиональной подготовки // Фундаментальные исследования. – 2014. – № 12–5. – С. 1078–1082.

6. Курзаева Л.В. Ситуационные тесты в системе оценки результатов обучения личности (на примере ИТ-направлений подготовки) // Научные труды SWorld. – 2013. – Т. 16. – № 3. – С. 61–63.

7. Овчинникова И.Г. Оценка эффективности образования личности вуза / И.Г. Овчинникова, В.А. Беликов, Л.В. Курзаева // Социальное партнерство в профессиональном образовании: материалы всероссийской науч.-практ. конф., Магнитогорск, 12 янв. 2010 г. – Магнитогорск: МГППК, 2010. – С. 178–187.

8. Чусавитина Г.Н. Е.В. Гридина Подготовка будущих учителей к использованию автоматизированных информационных технологий в педагогической диагностике: монография. – Магнитогорск: Изд-во Магнитогорск. гос. ун-та, 2005. – 242 с.

9. Чусавитина Г.Н. Развитие компетенций научно-педагогических кадров по обеспечению информационной безопасности в икт-насыщенной среде // Спрос и предложение на рынке труда и рынке образовательных услуг в регионах России. – 2011. – С. 338–345.

10. Чусавитина Г.Н. Применение интегративных механизмов при подготовке будущих учителей в области обеспечения информационной безопасности // Вестник компьютерных и информационных технологий. – 2010. – № 5. – С. 49–54.

11. Чусавитина Г.Н., Чусавитин М.О. Модель подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде // Новые информационные технологии в образовании: материалы Международной научно-практической конференции. – 2012. – С. 519–521.

12. Чусавитина Г.Н. Формирование компетентности будущих учителей в области обеспечения информационной безопасности // Вестник Московского государственного областного университета. Серия: Открытое образование. – 2006. – № 1. – С. 92–97.