УДК 378.1 + 002.004:004.052
ББК Ч448.44

ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РАЗВИТИЯ УПРАВЛЕНЧЕСКОЙ КОМПЕТЕНЦИИ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОБЛАСТИ КАДРОВОЙ БЕЗОПАСНОСТИ

А.А. Томилов
Южно-Уральский государственный университет, г. Челябинск

Обострение противоречий между потребностью современной практики защиты информации в специалистах, способных управлять кадровой безопасностью организации, и недостаточным использованием возможностей вуза в развитии этой компетенции у выпускников образовательного направления «Информационная безопасность» определяет актуальность темы исследования. Цель статьи – выявить педагогические условия развития управленческой компетенции специалиста по защите информации в области кадровой безопасности. Для достижения поставленной цели были использованы методы анализа теоретических и практических предпосылок; анализ законодательных и нормативно-правовых документов в сфере высшего образования, системный анализ процесса проектирования образовательного процесса, направленного на решение поставленной проблемы. Результатом статьи являются выявленные педагогические условия развития управленческой компетенции будущего специалиста по защите информации в области кадровой безопасности. Научная новизна статьи состоит в определении педагогических условий развития управленческой компетенции специалиста по защите информации в области кадровой безопасности организации и направлений их реализации на основе определенного понятия этой компетенции. Практическая значимость результатов, изложенных в статье, заключается в возможности их внедрения в процесс подготовки специалистов по защите информации в вузе.

Ключевые слова: защита информации, кадровая безопасность, специалист, управленческая компетенция, педагогические условия.

Человек является субъектом экономической жизни, поэтому человеческие ресурсы и человеческий капитал активно изучаются с 80-х годов XX века. Люди рассматриваются как основное конкурентное преимущество компании, которое необходимо развивать, мотивировать и стимулировать для достижения стратегических целей компании.

Большое значение человеческим ресурсам уделяется в сфере информационной безопасности, в которой человек рассматривается как главный источник угроз защищаемой информации. Федеральные государственные образовательные стандарты высшего профессионального образования по направлению «Информационная безопасность» предполагают наличие у специалистов по защите информации компетенций, связанных с оценкой рисков, в том числе кадровых. Так, выпускники специальности 090302 «Информационная безопасность телекоммуникационных систем» должны обладать способностью прогнозировать, ранжировать, моделировать информационные угрозы телекоммуникационных систем и оценивать уровни риска (ПК-21); специальности 090303 «Информационная безопасность автоматизированных систем» – способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14); специальности 090305 «Информационно-аналитические системы безопасности» – способностью выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-26). Особо пристальное внимание работе с людьми должны уделять выпускники специальности 090915 «Безопасность информационных технологий в правоохранительной сфере»: они должны обладать способностью формировать и реализовывать комплекс мер по обеспечению безопасности информации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1); способностью участвовать в пресечении и раскрытии правонарушений и преступлений в качестве специалиста (ПК-10); способностью осуществлять мероприятия по информацион-

но-психологическому обеспечению правоохранительной деятельности; применять при решении профессиональных задач психологические методы, средства и приемы (ПК-12); способностью реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений (ПК-13); способностью выявлять и содействовать пресечению коррупционных проявлений в служебном коллективе (ПК-16); способностью составлять обзоры по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности (ПК-34).

Очевидно, что формирование и развитие названных компетенций у будущих специалистов по защите информации требуют немалых усилий у выпускающих кафедр. Тем более что длительное время защита информации отождествлялась исключительно с техническими проблемами. Между тем, информационная безопасность имеет междисциплинарный характер, что обусловливает наличие у будущих специалистов по защите информации управленческой компетенции в области кадровой безопасности и выделение определенных педагогических условий ее развития в процессе обучения в вузе.

Управленческую компетенцию специалиста по защите информации в области кадровой безопасности мы определили как интегральное свойство его личности, обеспечивающее способность к деятельности по определению целей, выбору способов влияния и оказания его на сотрудников организации для развития человеческого капитала организации с целью обеспечения конфиденциальности, целостности и доступности информации в условиях динамики кадровых угроз и уязвимостей. Развитие этой компетенции предполагает процесс количественных и качественных изменений метологического и объектно-содержательных компонентов, выделенных нами на основе концепции понятия управленческой компетенции специалиста по защите информации Л.В. Астаховой [6]. Методологический компонент отражает сущность управления кадровой безопасностью: информационная и информационно-аналитическая компетенции, которые позволяют анализировать кадровые риски в организации, дают «ключ» к управлению человеческим капиталом организации на основе концепции его «защищенного развития». Объектно-содержательные компоненты отражают способность специалиста по защите информации оказывать влияние на различные объекты управления кадровой безопасностью и включают в себя: а) компетенции администратора (способности осуществлять административные функции управления: планирование, организацию, контроль процесса работы с кадрами для нейтрализации кадровых рисков и развития человеческого капитала организации); б) многоуровневые компетенции (способности оказывать влияние как на внутреннюю, так и на внешнюю среду: стратегическое управление кадровой безопасностью, управление инновациями (в том числе автоматизацией) в области работы с персоналом, управление изменениями человеческого капитала организации; в) компетенции управления собственной эффективностью как сотрудника организации (способности к самодиагностике, самоорганизации, саморазвитию, в том числе к развитию своего человеческого капитала: информационного мировоззрения и культуры информационной безопасности и пр.).

Согласно обоснованной структуре управленческой компетенции в области кадровой безопасности к педагогическим условиям ее развития мы относим следующие:

1) обучение студентов технологиям деятельности по обеспечению кадровой безопасности, соответствующим амбивалентному характеру парадигмы «защищенного развития» кадровых ресурсов организации;

2) организацию самодиагностики человеческого капитала студентов в учебном процессе в вузе;

3) использование в учебном процессе инновационных автоматизированных технологий оценки кадровых уязвимостей информационной безопасности организации.

Именно эти педагогические условия обеспечивают формирование такого целостного личностного качества, как управленческая компетенция специалиста по защите информации в области кадровой безопасности, которое сегодня является профессионально необходимым.

Первое педагогическое условие – обучение студентов технологиям деятельности по обеспечению кадровой безопасности, соот-

ветствующим амбивалентному характеру парадигмы «защищенного развития» кадровых ресурсов организации.

Предлагаемые в научной литературе трактовки сущности кадровой безопасности основаны на защите от кадровых угроз, или – на парадигме защищенности. Однако кроме данной парадигмы под влиянием социогуманитарной трансформации общества и интенсивных процессов информационного развития человечества четко проявилась еще одна парадигма безопасности – парадигма развития. На этот факт в контексте изучения информационной безопасности обратила внимание Л.В. Астахова [2]. Если предпосылкой обеспечения безопасности в рамках парадигмы защищенности является определение угроз безопасности, на устранение которых и направляется деятельность, то парадигма развития базируется не столько на существовании, т. е. борьбе с опасностями, сколько на развитии собственных внутренних сил. В настоящее время наблюдается устойчивая тенденция смещения акцентов в деятельности по обеспечению безопасности с парадигмы защищенности на парадигму развития. Появился концепт «безопасность через развитие», лежащий в основе целого ряда официальных документов, направленных на обеспечение разных видов безопасности Российской Федерации: «Стратегия национальной безопасности Российской Федерации» (2009), «Доктрина информационной безопасности Российской Федерации» (2000), «Стратегия развития информационного общества в Российской Федерации» (2008) и др. В этих документах акценты сделаны именно на проблемах развития.

В контексте разговора о кадровой безопасности организации весьма актуален вывод о том, что система, к каковой относится любая организация, не может быть жизнеспособной, только сохраняя достигнутое, без изменений и развития, поэтому парадигма защищенности в гипертрофированной форме в действительности не укрепляет безопасность, а разрушает ее. Поскольку источник развития находится вовне, развитие приобретает искусственный характер противопоставления иному – догнать и перегнать, добыть и сделать больше и т. п. В результате организация и ее сотрудники развивают не свои внутренние силы, а лишь свое противопоставление опасностям.

И наоборот – только самоутверждение, постоянное изменение субъекта без сохранения основы системы ставит под удар существование последней. Мы согласны с Л.В. Астаховой в том, что две парадигмы – защищенности и развития – должны не исключать, а дополнять друг друга. Современная тенденция – формирование методологии развития и ее гармоничное слияние с методологией защищенности. На стыке двух парадигм безопасности рождается одна – парадигма «защищенного развития» [2].

Поэтому кадровая безопасность должна изучаться будущими специалистами по защите информации в вузе в рамках дисциплины «Организационная защита информации» с позиций именно этой, интегративной парадигмы – парадигмы защищенного развития. Следовательно, система кадровой безопасности имеет двуединую, амбивалентную цель: обеспечение защищенности организации от кадровых угроз и развитие ее человеческого капитала. А это значит, что будущие специалисты по защите информации должны хорошо освоить не только технологии организации моделирования кадровых угроз, но и использования в организационной защите информации стратегического менеджмента персонала, экономики персонала [9, 10], психологии, педагогики и др. И для этого они должны также обучаться информационно-аналитическим технологиям как методологическому инструменту управления кадровой безопасностью.

Второе педагогическое условие – организация самодиагностики человеческого капитала студентов в учебном процессе в вузе.

Аксиомой в науке является факт, что человеческий капитал – решающий фактор производства новых товаров и услуг, который позволяет оптимизировать все бизнес-процессы и, как результат, имеет свой денежный эквивалент. Н.Н. Шаш определяет человеческий капитал организации как запас знаний, навыков и опыта персонала (в форме интеллектуальных способностей и практических навыков, полученных в процессе обучения и практической деятельности), который становится источником создания и распространения различного типа инноваций (продуктов, технологий, интеллектуальных моделей), приносит организации доход в виде прибыли; поддается измерению и является базовым для формирования рыночного, структурного и потребительского капитала, вместе с которы-

ми образует интеллектуальный капитал организации [11]. В связи с этим составной частью управления кадровой безопасностью должно стать управление развитием человеческого капитала организации, процесс которого включает совокупность воздействий, направленных на эффективное функционирование и увеличение стоимости не только самого человеческого капитала организации, но и его производных форм: рыночного, структурного и потребительского в контексте целей и стратегии конкретной организации. Наиболее сложным для специалиста по защите информации организации является последняя составляющая, связанная с оценкой человеческого капитала. В науке уже разработаны различные подходы к оценке человеческого капитала, которыми также должны владеть будущие специалисты по защите информации, осуществляющие деятельность по обеспечению кадровой безопасности. Однако в экономике защиты информации эти вопросы не разработаны.

Для освоения технологий оценки человеческого капитала в целях обеспечения информационной безопасности целесообразно организовывать самодиагностику человеческого капитала студентов в учебном процессе в рамках изучения курсов «Экономика защиты информации», «Кадровая безопасность». Структура диагностической программы должна строиться на различных методах оценки человеческого капитала. К ним относятся:

1. Метод оценки человеческого капитала на основе подсчета затрат на человеческий капитал: заработную плату, премии, повышение квалификации.

2. Метод определения первоначальных и восстановительных издержек на персонал. Данный метод рассматривает затраты фирмы, связанные с приобретением и заменой персонала, а не с его содержанием.

3. Метод измерения индивидуальной стоимости работника. В рамках данного метода учитывается ценность работника с учетом вероятности того, что он останется работать в организации в течение какого-то времени, определяющая ожидаемую реализуемую стоимость. Ожидаемая реализуемая стоимость, в свою очередь, состоит из двух элементов: ожидаемой условной стоимости и вероятности продолжения работы в организации.

4. Затратный метод, основанный на стоимостной оценке величины человеческого капитала, исходя из определения трех основных групп затрат, связанных с человеческим капиталом: фонда оплаты труда, затраты на интеллектуальный капитал и «капитал здоровья».

5. Сравнительный метод. Суть сравнительного метода состоит в выявлении различий между объектом оценки и аналогами.

6. Принцип капитализации будущих доходов – самый распространенный, когда величина человеческого капитала определяется экономическим эффектом от его использования, т. е. совокупным доходом. Дисконтируемая сумма всех будущих доходов составляет величину применяемого капитала.

7. Метод управленческой добавленной стоимости (УДС) заключается в измерении вклада ключевого управленческого персонала в добавленную стоимость предприятия.

8. Экспертный метод или метод качественной оценки. Сущность метода заключается в том, что оценке подвергаются качественные показатели, характеризующие как индивидуальные особенности конкретного работника, так и свойства работников компании в совокупности [8].

Целесообразной для образовательного процесса видится нам организация сравнительного анализа валидности названных методов, а также мониторинга показателей человеческого капитала как на разных этапах обучения студента в вузе, так и в различных профессиональных ролях.

Реализовать это педагогическое условие можно в форме виртуального предприятия с развернутой организационной структурой и штатным расписанием, в котором все должности должны занимать студенты группы. Целесообразно организовать самодиагностику человеческого капитала всех «сотрудников» виртуального предприятия вначале в рамках дисциплины «Экономика защиты информации», а в следующем семестре – в рамках дисциплины «Кадровая безопасность» (сначала в тех же, а затем – в других функциональных ролях).

Наиболее объективно оценить человеческий капитал студенты могут именно в процессе самодиагностики. Выявление динамики собственного уровня человеческого капитала позволит студентам повысить свою конкурентоспособность в стенах вуза до начала профессиональной деятельности, выбрать наиболее привлекательные функциональные роли, в которых студент имеет наилучшие показа-

тели человеческого капитала, а также корректировать его отдельные показатели.

Третье педагогическое условие – использование в учебном процессе инновационных автоматизированных технологий оценки кадровых уязвимостей информационной безопасности организации.

Самой сложной проблемой оценки кадровых рисков, уязвимостей и кадровой безопасности являются сложности формализации «человеческого фактора». Именно поэтому в науке тормозились разработки методов этой оценки, а процесс не поддавался автоматизации. В настоящее время многое изменилось. В практике управления персоналом используются программные средства. В сфере защиты информации также разработаны методы оценки кадровых уязвимостей информационной безопасности организации [1, 3], предприняты попытки автоматизации оценки кандидата на вакантную должность для обеспечения информационной безопасности организации [5], а также многофакторной оценки ее кадровой безопасности [4] и др.

Результатом автоматизации многофакторной оценки кадровых уязвимостей информационной безопасности, которая была разработана на основании основных этапов жизненного цикла деятельности по обеспечению кадровой безопасности организации, стал разработанный программный продукт, который позволяет: при приёме на работу обращать внимание не только на профессиональные компетенции соискателя, но и на его личностные характеристики; после его утверждения на должность – поддерживать должный уровень профессиональных знаний; при увольнении – корректно оценить его психологическое состояние [4]. Знакомство будущих специалистов по защите информации с названными и подобными программными продуктами в рамках профессиональных дисциплин, будет способствовать не только развитию их управленческой компетенции в области кадровой безопасности, но и развивать их инновационную культуру. Кроме традиционных лабораторных работ по названным программным продуктам, целесообразно выполнение студентами самостоятельной учебно-научной исследовательской работы по разработке собственных методов оценки кадровой безопасности и их автоматизации.

Таким образом, обоснованные педагогические условия развития управленческой компетенции будущих специалистов по защите информации в области кадровой безопасности организации связаны со структурой этой компетенции, а также с содержанием, организацией и условиями образовательного процесса в вузе. К ним относятся: 1) обучение студентов технологиям деятельности по обеспечению кадровой безопасности, соответствующим амбивалентному характеру парадигмы «защищенного развития» кадровых ресурсов организации; 2) организация самодиагностики человеческого капитала студентов в учебном процессе в вузе; 3) использование в учебном процессе инновационных автоматизированных технологий оценки кадровых уязвимостей информационной безопасности организации. Их реализация требует междисциплинарных знаний в области безопасности не только студентов, но и преподавателей.

Литература

1. Астахова, Л.В. Кадровые уязвимости информационной безопасности организации: методика оценки / Л.В.Астахова // Безпека інформації. – 2013. – Т. 20, № 2. – С. 133–138.

2. Астахова, Л.В. Парадигмы безопасности и безопасность как парадигма в XXI веке / Л.В. Астахова // Механика и процессы управления: Труды XXXVIII Уральского семинара. – Екатеринбург: Изд-во УрО РАН, 2008. – Т. 2. – С. 105–116.

3. Астахова, Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации / Л.В. Астахова // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление и радиоэлектроника». – 2013. – Т. 13, № 1. – С. 79–83.

4. Астахова, Л.В. Автоматизация многофакторной оценки кадровых уязвимостей информационной безопасности / Л.В. Астахова, В.А. Ефремов, А.И. Митькин // Вестник УрФО Безопасность в информационной сфере. – 2014. – № 4. – С. 49–53.

5. Астахова, Л.В. Автоматизация оценки кандидата на вакантную должность для обеспечения информационной безопасности организации / Л.В. Астахова, О.О. Землянская, В.А. Ефремов // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 1. – С. 34–38.

6. Астахова, Л.В. Управленческая компетенция специалиста по защите информации: монография / Л.В. Астахова. – Челябинск: Издат. центр ЮУрГУ, 2015. – 99 с.

7. Астахова, Л.В. Развитие информационно-аналитических компетенций студентов в вузе / Л.В. Астахова, А.Е. Трофименко // Вестн. Челяб. гос. пед. ун-та. – 2011. – № 12. – С. 16–23.

8. Кастрюлина, Ю.М. Анализ методов оценки величины человеческого капитала хозяйствующих субъектов / Ю.М. Кастрюлина // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». – 2013. – № 1. – С. 19.

9. Одегов, Ю.Г. Экономика персонала. Ч. I: Теория / Ю.Г. Одегов, Г.Г. Руденко. – М.: Изд-во «Альфа-Пресс», 2009. – 1056 с.

10. Одегов, Ю.Г. Экономика персонала. Ч. II: Практика / Ю.Г. Одегов, Г.Г. Руденко, А.А. Федченко. – М.: Изд-во «Альфа-Пресс», 2009. – 1312 с.

11. Шаш, Н.Н. Развитие человеческого капитала организации: теория, методология: дис. … д-ра эконом. наук / Н.Н. Шаш. – Саратов, 2006. – 438 с.

Томилов Александр Александрович, аспирант кафедры безопасности информационных систем, Южно-Уральский государственный университет (Челябинск), tomilov62@yandex.ru.

Поступила в редакцию 10 апреля 2015 г.

PEDAGOGICAL CONDITIONS OF COMPETENCE DEVELOPMENT OF A SPECIALIST IN DATA SECURITY IN THE AREA OF PERSONNEL SECURITY

***A.A. Tomilov**, South Ural State University, Chelyabinsk, Russian Federation, tomilov62@yandex.ru*

The aggravated contradiction between the need in professionals in data security capable of managing personnel security of the organization and the insufficient use of opportunities of the university in the development of the student competence in the area of data security determines the relevance of the research. Theoretical analysis of the literature, first-hand experience, the analysis of legislative documents and documents in the sphere of higher education were used to identify the pedagogical conditions of the development of competence of a specialist in information security in the field of personnel security. Based on the competence described the pedagogical conditions of the development of competences of a future specialist in data security in the area of personnel security were identified together with the directions of their implementation. The results can be used in the educational process of specialists preparation in data security.

Keywords: data security, personnel security, specialist, competence, pedagogical conditions.

References

1. Astakhova L.V. [Human Vulnerability Information Security: Assessment Methodology]. *Ukrainian Scientific Journal of Information Security*, 2013, vol. 20, no. 2, pp. 133–138. (in Ukr.)

2. Astakhova L.V. [Paradigms Safety and Security as a Paradigm of the XXI Century]. *Mekhanika i protsessy upravleniya: Trudy* XXXVIII *Ural'skogo seminara. T. 2* [Mechanics and Control: Transactions of the Ural XXXVIII Seminar. Vol. 2]. Ekaterinburg, 2008, pp. 105–116. (in Russ.)

3. Astakhova L.V. [The Problem of Identification and Evaluation of Human Vulnerability Information Security]. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control & Radioelectronics*, 2013, vol. 13, no. 1, pp. 79–83. (in Russ.)

4. Astakhova L.V., Efremov V.A., Mit'kin A.I. [Automation Multifactorial Assessment of Human Vulnerability Information Security]. *Bulletin of the Ural Federal District. Information Security*, 2014, no. 4, pp. 49–53. (in Russ.)

5. Astakhova L.V., Zemlyanskaya O.O., Efremov V.A. [Automation of an Estimation of the Candidate for the Vacant Post of Information Security Organization]. *Bulletin of the Ural Federal District. Information Security*, 2014, no. 1, pp. 34–38. (in Russ.)

6. Astakhova L.V. *Upravlencheskaya kompetentsiya spetsialista po zashchite informatsii* [Managerial Competence of Information Security Specialists]. Chelyabinsk, South Ural St. Univ. Publ., 2015. 99 p.

7. Astakhova L.V., Trofimenko A.E. [The Development of Information and Analytical Competences of Students in High School]. *Bulletin of the Chelyabinsk State Pedagogical University*, 2011, no. 12, pp. 16–23. (in Russ.)

8. Kastryulina Y.M. [The Analysis Methods for Assessing the Value of the Human Capital of Business Entities]. *Scientific Journal ITMO. Ser. Economy and Environmental Management*, 2013, no. 1, pp. 19. (in Russ.)

9. Odegov Yu.G., Rudenko G. *Ekonomika personala. Chast' I. Teoriya* [Economy Staff. Part I. Theory]. Moscow, Alpha-Press Publ., 2009. 1056 p.

10. Odegov Yu.G., Rudenko G.G., Fedchenko A.A. *Ekonomika personala. Chast' II. Praktika* [Economy Staff. Part II. Practice]. Moscow, Alpha-Press Publ., 2009. 1312 p.

11. Shash N.N. *Razvitie chelovecheskogo kapitala organizatsii: teoriya, metodologiya.* Dis. dokt. ekonom. nauk [The Development of Human Capital of the Organization: the Theory, Methodology. Diss. Doct. (Economy)]. Saratov, 2006. 438 p.

Received 10 April 2015

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Томилов, А.А. Педагогические условия развития управленческой компетенции специалиста по защите информации в области кадровой безопасности / А.А. Томилов // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». – 2015. – Т. 7, № 3. – С. 95–101.

FOR CITATION

Tomilov A.A. Pedagogical Conditions of Managerial Competence Developement of a Specialist in Data Security in the Area of Personnel Security. *Bulletin of the South Ural State University. Ser. Education. Educational Sciences.* 2015, vol. 7, no. 3, pp. 95–101. (in Russ.)