Теория и методика профессионального образования

УДК 004.056 + 378.016:004.056
ББК Ч448.043 + Ч448.02
DOI: 10.14529/ped160203

ДОВЕРИЕ К БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КАК ОБЪЕКТ ИЗУЧЕНИЯ БУДУЩИМИ СПЕЦИАЛИСТАМИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Л.В. Астахова
Южно-Уральский государственный университет, г. Челябинск

Выявлена актуальность углубления знаний доверия к безопасности информационных технологий будущими специалистами по защите информации в вузе. Обоснованы императивы расширения границ и углубления содержания объектов изучения студентами вуза системы деятельности по оценке доверия к безопасности информационных технологий: целей, субъектов, объектов, методов, процессов и их результатов. К ним отнесены: 1) развитие организации и ее сотрудников как цель достижения безопасности информационной системы, доверие к которой оценивается; 2) субъект доверия к безопасности информационной системы, его компетенции, влияющие на результат оценки доверия; 3) социотехнический характер информационной системы, предполагающий оценку не только ее технических компонентов, но и доверия к пользователям как к неотъемлемой части этой системы; 4) не только технические, но и гуманитарные методы решения проблемы доверия к информационной безопасности; 5) не только процессы деятельности по обеспечению доверия к безопасности информационной системы, но и все остальные системные компоненты этой деятельности, в том числе ее результаты. Выявлены и обоснованы педагогические условия внедрения этих императивов в практику: проблемная ориентация учебно-методического обеспечения дисциплины «Управление информационной безопасностью»; углубление междисциплинарных связей этой дисциплины с философией, социологией, экономикой, психологией, педагогикой; развитие инновационной культуры студентов для моделирования нового стандарта по критериям оценки доверия и его внедрению в практику, для разработки программных продуктов, способных реализовать разработанные гуманитарно-оценочные процедуры.

Ключевые слова: специалист по защите информации, компетенция, доверие, информационная технология, информационная безопасность, оценка, педагогические условия.

Введение

Актуальность изучения в вузе доверия к безопасности информационных технологий обусловлена усиливающимися угрозами и ростом инцидентов информационной безопасности во всем мире. При этом подготовка будущих специалистов по защите информации в вузах осуществляется на основе международного стандарта ISO/IEC 15408-3:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3. Security assurance components», который не отражает современных гуманитарных аспектов проблемы. Они обусловлены динамикой научного знания о целях информационной безопасности, концепции защищенного развития, о трансформации технических систем в социотехнические, о кадровой безопасности и др. Этим обусловлена актуальность проблемы статьи.

1. Объекты изучения доверия к информационной безопасности в университете

Недостаточный учет человеческого фактора в международном стандарте [1] требует от высшего профессионального образования расширения границ объектов изучения в вузе будущими специалистами по защите информации. В их число преподаватель вуза, наряду с названными в стандарте, должен включать:

– развитие организации и ее сотрудников как цель достижения безопасности информационной системы, доверие к которой оценивается;

– субъект доверия к безопасности информационной системы, его компетенции, влияющие на результат оценки доверия;

– социотехнический характер информационной системы, предполагающий оценку не только ее технических компонентов, но и доверия к пользователям как к неотъемлемой части этой системы;

– не только технические, но и гуманитарные методы решения проблемы доверия к информационной безопасности;

– не только процессы деятельности по обеспечению доверия к безопасности информационной системы, но и все остальные системные компоненты этой деятельности, в том числе ее результаты.

Рассмотрим эти объекты изучения подробнее.

Развитие организации и ее сотрудников как цель достижения безопасности информационной системы, доверие к которой оценивается. Сущность современной концепции защищенного развития объекта заключается в следующем. Для обеспечения информационной безопасности объекта недостаточно только защищенности от всех возможных угроз. Гиперболизация внимания на угрозах и защите от них может привести к неоправданной изоляции объекта от внешней среды, к блокированию информационного взаимообмена с ней. Это опасно тем, что возникают негативные, застойные явления в существовании объекта. Для предотвращения этих явлений следует стимулировать еще один процесс – развитие.

Развитие объекта всегда сопровождается активным информационным взаимодействием с другими объектами. В результате происходит информационное взаимообогащение объектов. Обнаружена интересная тенденция: превышение объемов исходящего информационного потока над входящим свидетельствует о лидерстве этого объекта, о его доминировании не только в информационном, но и геополитическом, экономическом пространстве, а значит – о его более высоком уровне развития. Так, например, сильные, высокоразвитые государства, являющиеся влиятельными распорядителями информационного пространства, обладают гораздо более высоким уровнем информационной безопасности [2]. Поэтому мы можем утверждать, что целью информационной безопасности организации является не только защита информации в этой организации, но и ее устойчивое информационное развитие. Это касается и сотрудников организации.

Субъект доверия к безопасности информационной системы, его компетенции, влияющие на результат оценки доверия. Общеизвестно, что результат доверия в значительной степени зависит от субъекта этого процесса. В сфере информационной безопасности этим субъектом выступает специалист по защите информации. Однако, к сожалению, в стандарте ISO/IEC 15408-3:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3. Security assurance components» его оценка не предусмотрена.

Качество аудита определяется компетентностью аудитора, в которую входят личностные качества. Этот вопрос отражен в ГОСТ Р ИСО/МЭК 27007-2014 – Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности [3]. Названный стандарт определяет методику определения компетентности аудиторов системы менеджмента информационной безопасности.

Исходя из содержания п. 7.2.2 стандарта, аудиторы должны проявлять определенные личные качества во время проведения аудита. Они включают в себя: этичность, открытость и непредубежденность, дипломатичность, наблюдательность, восприимчивость, упорство, решительность, самостоятельность, принципиальность, высокую культуру поведения, умение сотрудничать и работать с людьми и др. Наличие этих личных качеств можно использовать для оценки доверия к специалисту по защите информации как субъекту доверия к безопасности информационной системы.

Социотехнический характер информационной системы, предполагающий оценку не только ее технических компонентов, но и доверия к пользователям как к неотъемлемой части этой системы. К особенностям современной инженерной практики относится ее эволюция от классической инженерной к системотехнической деятельности и далее – к социотехническому, гуманитарному проектированию. Это относится и к проектированию информационных систем.

Социотехническое гуманитарное проектирование, по сравнению с классической инженерной деятельностью, предполагает определенную гуманитарную диагностику и экспертизу информационной системы. Его задача – не просто создать информационную систему, а обеспечить ее нормальное функционирование в организации. Здесь главное внимание уделяется не компьютерам, а человеку и его деятельности, её социальным и психологическим аспектам, новым технологиям. Поэтому социотехническое проектирование выходит за пределы традиционной схемы «наука-инженерия-производство». Оно замыкается на самые разнообразные виды социальной практики, в том числе на обучение персонала, где классическая инженерная установка перестает действовать. Все это ведет к тому, что информационная система становится самостоятельной сферой современной культуры. Этого нельзя не учитывать в процессе обеспечения информационной безопасности организации. Пользователи – органическая часть информационной системы. Поэтому в процессе оценки доверия к безопасности информационных технологий следует оценивать и доверие к пользователям информационной системы организации.

Технические и гуманитарные методы решения проблемы доверия к информационной безопасности. Традиционно используются методы автоматизированного мониторинга доверия к безопасности информационных технологий. Включение сотрудников организации в число объектов изучения требует и расширения изучаемых методов решения этой проблемы. В этом случае необходимы гуманитарные методы обеспечения кадровой безопасности. Анализ существующих подходов к оценке человеческого фактора для снижения рисков информационной безопасности организации выявил междисциплинарный характер проблемы и слабую формализумость оценок человеческого фактора, что усложняет поиск ее решения. При этом определенный опыт изучения данной проблематики уже накоплен в отечественной науке. Так, в одной из моих публикаций обоснован метод оценки кадровых рисков на основе оценки индекса доверия как отношении культурных капиталов информационной безопасности индивида и организации [4]. Важнейшим показателем доверия к сотруднику является степень конвертации его культурного капитала в культурный капитал организации. Эти и другие методы должны осваивать студенты в процессе обучения в вузе для развития их профессиональных компетенций.

Процессы деятельности по обеспечению доверия к безопасности информационной системы и все остальные системные компоненты этой деятельности, в том числе результаты. В стандарте ISO/IEC 15408-3:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3. Security assurance components» акцент сделан на процессах оценки доверия к безопасности информационных технологий. Оценочные уровни доверия выделены также на основе оценки процессов. Однако необходимо, чтобы студенты вуза изучали результаты количественной и качественной оценки доверия ко всем системно-деятельностным элементам: объекту (информационной системе и ее пользователям), субъекту (специалисту по защите информации), процессам (согласно оценочным уровням доверия) и методам (технические и гуманитарные) оценки доверия, комплексному результату оценки доверия.

2. Педагогические условия освоения студентами деятельности по оценке доверия к информационной безопасности

Названные объекты требуют специфических педагогических условий организации образовательного процесса. К ним относятся: проблемная ориентация учебно-методического обеспечения дисциплины «Управление информационной безопасностью»; углубление междисциплинарных связей этой дисциплины с философией, социологией, экономикой, психологией, педагогикой; развитие инновационной культуры студентов для моделирования нового стандарта по критериям оценки доверия и его внедрению в практику, для разработки программных продуктов, способных реализовать разработанные гуманитарно-оценочные процедуры.

Проблемная ориентация учебно-методического обеспечения дисциплины «Управление информационной безопасностью» предполагает: создание онтологии проблемы оценки доверия к безопасности информационных технологий; проблемные формулировки тем лекций, семинаров и научных докладов на научно-практических конференциях; работу студентов под руководством преподавателя над решением этих проблем.

Углубление междисциплинарных связей этой дисциплины с философией, социологией, экономикой, психологией, педагогикой предполагает: включение в дисциплину «Управление информационной безопасностью» повторения философии техники, экономики защиты информации, теории человеческого и культурного капитала, теории информационно-психологической безопасности, педагогических технологий повышения осведомленности сотрудников в области информационной безопасности и др.

Развитие инновационной культуры студентов предполагает развитие их потребностей в совершенствовании теории и практики оценки доверия безопасности информационных технологий; задания по моделированию нового стандарта по критериям оценки доверия и его внедрению в практику; задания по разработке программных продуктов, способных реализовать разработанные гуманитарно-оценочные процедуры.

В ходе реализации педагогических условий каждый студент подготовил инновационный проект по кадровым рискам для его внедрения в практику, опубликовал результаты своей работе в научном журнале. Проекты были посвящены разработке классификации групп кадровых рисков для информационной системы, инновационных критериев их оценки. Например, в рамках дисциплины «Кадровая безопасность» студенческий научный коллектив разработал программное приложение для оценки культурного капитала пользователей информационной системы для обеспечения ее безопасности. В настоящее время оно внедряется в практике защиты информации.

Эксперимент показал, что реализация обоснованных педагогических условий позволяет развить у будущих специалистов по защите информации управленческую компетенцию в данной области. Управленческая компетенция будущего специалиста по защите информации в области доверия к безопасности информационных технологий – это интегральное качество его личности, обеспечивающее способность оказывать влияние на уровень доверия к безопасности информационных систем, включая их пользователей, с применением технических и гуманитарных методов.

Заключение

Научная новизна статьи состоит в обосновании расширения границ и углубления содержания объектов изучения системы деятельности по обеспечению доверия: целей, субъектов, объектов, методов, процессов и их результатов. Теоретическая значимость исследования заключается в обогащении теории профессионального образования: в определении понятия управленческой компетенции будущего специалиста по защите информации в области доверия к безопасности информационных технологий; в обосновании специфических педагогических условий их внедрения. Результаты исследования имеют практическую значимость, поскольку обоснованные рекомендации по подготовке специалистов по защите информации в вузах внедрены автором в практику в Южно-Уральском государственном университете (Россия). Это способствовало повышению качества инженерного образования, развитию управленческой компетенции будущих инженеров, а также гуманитаризации их подготовки.

Литература

1. ISO/IEC 15408-3:2008 “Information technology – Security techniques – Evaluation criteria for IT security – Part 3. Security assurance components”. – http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413 (дата обращения: 5.03.2016).

2. Мир без границ – война без фронтов? – Челябинск: Изд-во ЮУрГУ, 2002. – 381 с.

3. ГОСТ Р ИСО/МЭК 27007-2014 – Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. – http://www.iso.org/iso/home/search.htm?qt=R++ISO+%2F+IEC+27007-2014&published=on&active_ tab=standards&sort_by=rel (дата обращения: 5.03.2016)

4. Astakhova, L.V. Information Security: Risks Related to the Cultural Capital of Personnel (Review) / L.V. Astakhova // Scientific and Technical Information Processing. – 2015. – Vol. 42, no. 2. – P. 41–52.

Астахова Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры безопасности информационных систем, Южно-Уральский государственный университет, г. Челябинск, lvastachova@mail.ru.

Поступила в редакцию 6 марта 2016 г.

DOI: 10.14529/ped160203

CREDIBILITY OF INFORMATION TECHNOLOGY SECURITY AS AN OBJECT OF STUDY FOR FUTURE SPECIALISTS IN INFORMATION SECURITY

***L.V. Astakhova**, lvastachova@mail.ru*
South Ural State University, Chelyabinsk, Russian Federation

The article reveals the necessity to increase the degree of assurance in the security of information technologies for future specialists. The reasons to study the evaluation system of assurance in security of information technologies are given. They are: 1) development of the organization and its employees as a goal to achieve information system security the credibility of which is estimated; 2) the credibility subject in the security of information systems, subject's competences affecting the result of the credibility evaluation; 3) socio-technical nature of the information system when the technical components are assessed as well as the information users both being integral parts of this system; 4) technical and human-oriented methods to provide credibility of an information system; 5) activities to ensure the credibility of the information system security and their results. The pedagogical conditions to implement the imperatives into practice are defined. They are: problem orientation of the subject "Information Security Management"; strengthening the interdisciplinary links with Philosophy, Sociology, Economics, Psychology and Pedagogy; development of innovative culture of students to model new standard evaluation criteria of credibility and its implementation into practice, which will be used to develop software implementing human-oriented evaluation procedures.

Keywords: *information security, competence, assurance, assessment, credibility, pedagogical conditions.*

References

1. *ISO / IEC 15408-3: 2008 "Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3. Security Assurance Components".* Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413 (accessed 5.03.2016).

2. *Mir bez granits – voyna bez frontov?* [World without Borders – a War without Fronts?]. Chelyabinsk, South Ural St. Univ. Publ., 2002. 381 p.

3. *GOST R ISO/MEK 27007-2014 – Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Rukovodstva po auditu sistem menedzhmenta informatsionnoy bezopasnosti* [GOST R ISO / IEC 27007-2014 "Information Technology. Methods and Means of Ensuring Safety. Guidelines for the Audit Information Security Management Systems"]. Available at: http://www.iso.org/iso/home/search.htm?qt=R++ISO+%2F+IEC+27007-2014&published=on&active_tab=standards&sort_by=rel (accessed 5.03.2016).

4. Astakhova L.V. Information Security: Risks Related to the Cultural Capital of Personnel (Review). *Scientific and Technical Information Processing*, 2015, vol. 42, no. 2, pp. 41–52. DOI: 10.3103/S0147688215020021

Received 6 March 2016

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Астахова, Л.В. Доверие к безопасности информационных технологий как объект изучения будущими специалистами по защите информации / Л.В. Астахова // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». – 2016. – Т. 8, № 2. – С. 19–23. DOI: 10.14529/ped160203

FOR CITATION

Astakhova L.V. Credibility of Information Technology Security as an Object of Study for Future Specialists in Information Security. *Bulletin of the South Ural State University. Ser. Education. Educational Sciences*. 2016, vol. 8, no. 2, pp. 19–23. (in Russ.) DOI: 10.14529/ped160203