УДК 004.056.53 Вестник УрФО № 2(32) / 2019, с. 52–59

Астахова Л. В.

DOI: 10.14529/secur190208

КАДРОВАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ: ОЦЕНОЧНЫЕ УРОВНИ ДОВЕРИЯ

В статье определено понятие «доверие к кадровой безопасности информационной системы», выделены две группы критериев оценки доверия к кадровой безопасности информационной системы для работодателя и работника: компетентностные и личностные критерии. Компетентностные критерии представлены уровнем осведомленности в области информационной безопасности и наличием документированных процедур мониторинга динамики культурного капитала организации; личностные критерии - уровнем конвертации культурного капитала сотрудников в культурный капитал организации; уровнем глубины оснований взаимного доверия работодателей и работников. На основе названных критериев обоснована многокритериальная классификация оценочных уровней доверия к кадровой безопасности информационной системы. Выделены семь оценочных уровней доверия к кадровой безопасности, которые соотносятся с семью оценочными уровнями доверия к информационным технологиям, закрепленными в международном стандарте ISO/IEC 15408-3:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components». Обоснована необходимость расширения содержания оценочных уровней доверия в названном стандарте для повышения безопасности информационных технологий.

Ключевые слова: *кадровая безопасность, информационная система, информационная безопасность, доверие, оценка, уровень, пользователь.*

Astakhova L. V.

HUMAN SECURITY INFORMATION SYSTEM: EVALUATING LEVEL OF CONFIDENCE

The article defines the concept of „trust in the personnel security of the information system", two groups of criteria for assessing the credibility of the personnel safety of the information system for the employer and employee are identified: competence and personal criteria. Competence criteria are represented by the level of awareness in the field of information security and the availability of documented procedures for monitoring the dynamics of the cultural capital of the organization; personal criteria - the level of converting the cultural capital of employees into the cultural capital of the organization; the depth of the bases of the mutual trust of employers and employees. On the basis of the above criteria, a multicriteria classification of the estimated levels of trust in the personnel security of the information system is grounded. There are seven estimated levels of confidence in personnel security that correspond to the seven esti-

mated levels of confidence in information technology as enshrined in the international standard ISO / IEC 15408-3: 2008 „Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components „. The necessity of expanding the content of estimated confidence levels in the named standard for increasing the security of information technologies is substantiated.

Keywords: *personnel security, information system, information security, trust, evaluation, level, user, Introduction.*

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02. A03.21.0011

Введение. В первом полугодии 2017 г. Аналитический центр InfoWatch зарегистрировал 925 случаев утечек конфиденциальной информации – на 10% больше, чем за аналогичный период 2016 года. В **56,3 %** случаев виновниками утечек информации были сотрудники компаний: настоящие или бывшие (50,6 % и 2,8 % соответственно); в 1,7 % - руководители; 1,2 % - подрядчики и системные администраторы [1]. Эти цифры свидетельствуют о том, что пользователь, или внутренний клиент, как важнейшее звено информационной системы серьезно недооценивается в практике обеспечения защиты информации. Это заключение подтверждают и результаты анализа сложившегося в мире подхода к достижению доверия к безопасности информационных систем. Стандарт ISO/IEC 15408-3:2008 "Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components" [2] и идентичный ему ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» [3] имеет существенный недостаток. В нем предпринята попытка решить проблему доверия к безопасности информационной системы как сугубо технической системы. Между тем, любая информационная система является сегодня социотехнической. В связи с этим безопасность информационной системы не может быть оценена без учета доверия к ее пользователям, а значит, - без использования научно-гуманитарных подходов.

Проблема доверия к социотехническим системам активно исследуется сегодня в экономике, социологии, психологии. Так, А.Б. Куприйченко включает в число основных структурных элементов модели к социотехническим системам доверие к различным категориям людей, обеспечивающим функционирование системы (создателям, организаторам, модераторам системы и другим заинтересованным сторонам) [4, С.435 –436]. По мнению B. Uzzi, на организационное доверие влияют три группы факторов: организационные факторы (характеристики организации) — структура, политика организации в отношении персонала, организационная культура; факторы отношений (характеристики ситуации) — первичное взаимодействие, ожидания, «стоимость обмена»; индивидуальные факторы (личностные характеристики субъекта доверия) — склонность к доверию, самоэффективность, ценности [5]. Однако в теории информационной безопасности доверию пользователю защищаемой информационной системы уделяется недостаточное внимание, хотя некоторые вопросы кадровой безопасности решаются на уровне стандартов [6] и даже на уровне автоматизации [7]. Противоречие между ростом числа утечек информации по вине пользователей информационных систем, с одной стороны, и игнорированием их пользователей в процессе оценки доверия к их безопасности, – с другой, обусловливает актуальность проблемы доверия к пользователю информационной системы как ее неотъемлемой части, а также разработки оценочных уровней доверия к кадровой безопасности информационной системы.

Доверие к кадровой безопасности информационной системы и критерии его оценки. Доверие к кадровой безопасности информационной системы мы определяем как субъективное взаимное ожидание руководства и сотрудников организации постоянства поддержания естественных и нравственных законов и доверительной ответственности (личностный компонент), а также компетентного исполнения действий в области информационной безопасности (компетентностный компонент) для обеспечения успешного функционирования и развития обоих

субъектов. Субъектная и объектная амбивалентность сформулированного понятия и анализ современных подходов к оценке доверия к социотехническим системам позволяет выделить две группы критериев оценки доверия, специфичные для работодателя и для работника: компетентностные и личностные.

Личностные критерии. Уровень конвертации культурного капитала сотрудников в культурный капитал организации (IDpers). Он обусловлен современными потребностями человека как субъекта хозяйственной жизни. Согласно исследованиям, приоритетными для человека в современной культуре и оказывающими наибольшее позитивное влияние на экономическое развитие являются ценности самореализации, духовности и поиска удовольствий [8]. Это требует изучения культурного капитала сотрудников и его реализации в организации. Исследование проблем оценки культурного капитала активно ведется в современной экономической науке [9 и др.]. Однако разработанная нами методика «отношений культурных капиталов» представляется наиболее эвристичной для оценки доверия к кадровой безопасности информационной системы. Основанная на выявлении индекса доверия как отношения культурных капиталов сотрудника в организации и вне ее, она позволяет осуществлять мониторинг названных капиталов и разрыва между ними, оценивать необходимые направления развития структурного капитала организации для снижения рисков информационной безопасности в отношении каждого сотрудника в любой период времени.

Индекс доверия к каждому сотруднику вычисляется по формуле как отношение двух выявленных показателей по каждому сотруднику:

$$Dpers = ICCISpers/corp : ICCISpers, \quad (1)$$

где: Dpers – индекс доверия сотрудника n;

ICCISpers/corp – корпоративный культурный капитал информационной безопасности сотрудника n в организации;

ICCISpers – индивидуальный культурный капитал информационной безопасности сотрудника вне организации;

Задача организации в процессе реализации цели обеспечения ее информационной безопасности – конвертировать сформированный индивидуальный культурный капитал сотрудника (пользователя ИС) в корпоративный культурный капитал [10, с.9].

Обоснованная методика позволяет решить одну из сложнейших проблем, связанных с мотивацией сотрудника, его субъективными взглядами и этико-моральными качествами, а не ограничиваться только уровнем профессионализма и характером персонала, [11]. Она дает возможность приблизиться к решению дилеммы «руководитель-работник» («Principal–agentproblem» или «agencydilemma»), которая возникает в том случае, когда работник (agent) выполняет какие-либо действия (принимает решения) от имени руководителя (principal), а руководствуется собственным мнением, мотивацией или своими интересами, а не работодателя [12]. Для решения проблемы ученые разработали принципы стимулирования компенсации работнику: информативности (максимума информации об обязанностях наемного рабочего и его компенсациях); интенсивности мотивации сотрудника (получение дополнительных доходов от дополнительных усилий сотрудника, его отзывчивость на стимулы мотивации); мониторинга интенсивности мотивации; эквивалентной компенсации интенсивности мотивации сотрудника [13.]. Данные принципы подчеркивают осознание необходимости достижения обратной связи работодателя и работника в процессе стимулирования последнего к реализации его культурного капитала.

Уровень глубины оснований взаимного доверия работодателей и работников (LDD). В зарубежных публикациях предлагается следующая классификация и характеристика оснований доверия: отсутствие доверия – на основе устрашения; низкое доверие – на основе расчета; доверительный уровень – на основе знаний; высокое доверие – на основе отношений; полное доверие – на основе идентификации; аутентичное доверие [14, 15, 16, 17.]. Чтобы избежать «агентских издержек» (agencycosts) [18], упомянутых выше, эксперты предлагают использовать комиссионное вознаграждение; вознаграждение, выплачиваемое в виде процента от прибыли; сдельную оплату труда; измерение производительности; указание перечня всех обязательств агента; угрозу увольнения агента [19]. Учитывая приведенную классификацию оснований доверия, заметим, что не каждая из названных мер может способствовать повышению доверия между работодателем и

сотрудником. Например, угроза увольнения агента - это устрашение, а потому - основание отсутствия доверия. Наиболее адекватный уровень доверия для сферы информационной безопасности начинается с доверия на основе отношений, поскольку взаимодействие является онтологической основой безопасности, в том числе информационной.

Компетентностные критерии. Уровень осведомленности в области информационной безопасности (LAP). Наиболее известными стандартами и рекомендациями по выстраиванию процесса повышения осведомленности являютя: PCI Council Best Practices for Implementing a Security Awareness Program, NIST Special Publication 800-50, ENISA The new users' guide: How to raise information security awareness, ГОСТ Р ИСО/МЭК ТО13335-3—2007 Методы и средства обеспечения безопасности, ISO/IEC TR 13335-3:1998 Раздел 10.3 Обучение персонала информационной безопасности, ISO 27001, COBIT 5 и др. Так, рекомендации ENISA включают 71 критерий осведомленности, которые можно укрупнить до 7 групп и привести их в соответствие со стандартными оценочными уровнями доверия к информационным технологиям.

Наличие документированных процедур мониторинга динамики культурного капитала организации, отражающее организационные меры по повышению доверия к кадровой безопасности информационной системы (DP). Индивидуальный и корпоративный культурные капиталы должны быть в организации объектами планирования, учета, контроля, оценки и совершенствования, а все эти процессы - документироваться. Это будет свидетельствовать об уровне осознания руководством важности вопросов работы с кадрами по использованию их знаний, умений, опыта и достижений для экономического роста предприятия и осведомленности об этом.

В результате анализа показателей по названным критериям можно увидеть уровень категориальной структуры персонала (LPR) и – уровень кадровых рисков. В любой организации есть четыре категории персонала, выделяемых в зависимости от результатов деятельности работников, от совокупности их знаний, умений и навыков, а также психофизиологических особенностей: персонал-капитал, персонал-ресурс, персонал и кадры. От структурного отношения этих категорий зависит уровень возможного кадрового риска: высокий, средний и низкий [20]. Чем больше процедур реализовано в организации, тем больше в ней персонала категории «персонал-капитал», способной повлиять на экономический рост, и ниже уровень кадровых рисков.

Многокритериальная классификация оценочных уровней доверия к кадровой безопасности информационной системы. Названные критерии могут быть положены в основу многокритериальной классификации оценочных уровней доверия к кадровой безопасности информационной системы. Любой из уровней может быть описан с помощью модели:

ОУД КБ=IDpers+LDD+LAP+DP+LPR, (2)

где: ОУД КБ – оценочный уровень доверия к кадровой безопасности;

IDpers – индекс доверия сотрудника к организации (степень конвертации его КК в корпоративный КК);

LDD – уровень глубины оснований взаимного доверия;

DP – документированные процедуры мониторинга культурного капитала организации;

LPR – уровень кадровых рисков по соотношению категорий персонала;

LAP – уровень осведомленности персонала в области информационной безопасности.

Каждый из семи оценочных уровней характеризуется показателями по каждому из выделенных критериев доверия (Табл.1). Так, например:

ОУД КБ7=(IDpers=0,8-1)+(LDD=Аутентичное доверие)+LAP=7)+(DP=6)+(LPR=Низкий) (3)

Многокритериальная классификация оценочных уровней доверия к кадровой безопасности информационной системы должна быть объектом изучения будущими специалистами по защите информации. Подробнее педагогический опыт в этом направлении охарактеризован нами в [21]. В качестве педагогических условий освоения студентами доверия к кадровой безопасности информационной системы мы обосновали: проблемную ориентацию учебно-методического обеспечения дисциплины «Управление информационной безопасностью»; углубление междисциплинарных связей этой дисциплины с философией, социологией, экономикой, психологией, педагогикой; развитие инновацион-

Таблица 1

Многокритериальная классификация оценочных уровней доверия к кадровой безопасности информационной системы

Характеристика ОУД КБ № ОУД КБ	Индекс конвертации индивидуального КК в корпоративный / IDpers	Категории персонала	Уровень глубины оснований взаимного доверия/LDD	Уровень осведомленности /LAP	Наличие документированных процедур мониторинга КК/DP	Уровень кадрового риска / LPR
1	0,2	кадры	Отсутствие доверия – на основе устрашения	1	-	высокий
2	0,3			2	1	
3	0,4	персонал	Низкое доверие – на основе расчета	3	2	
4	0,5		Доверительный уровень – на основе знаний	4	3	средний
5	0,6	персонал-ресурс	Высокое доверие – на основе отношений	5	4	
6	0,7	персонал-капитал	Полное доверие – на основе идентификации	6	5	низкий
7	0,8 - 1		Аутентичное доверие	7	6	

ной 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, и др.

Заключение. Рост числа инцидентов информационной безопасности по вине персонала организации требует совершенствования методов оценки доверия к безопасности информационных систем за счет усиления их кадровой безопасности. Однако существующие методики оценки доверия к безопасности информационной системы не учитывают социотехнический характер информационной системы и современные гуманитарные подходы к оценке доверия к ним.

В статье определено понятие «доверие к кадровой безопасности информационной системы», как субъективное взаимное ожидание руководства и сотрудников организации постоянства поддержания естественных и нравственных законов и доверительной ответственности (личностный компонент), а также компетентного исполнения действий в области информационной безопасности (компетентностный компонент) для обеспечения успешного функционирования и развития обоих субъектов.

Субъектная и объектная амбивалентность сформулированного понятия и анализ современных подходов к оценке доверия к социотехническим системам позволил выделить две группы критериев оценки доверия к кадровой безопасности информационной системы и для работодателя, и для работника: компетентностные и личностные критерии. Компетентностные критерии представлены уровнем осведомленности в области информационной безопасности и наличием документированных процедур мониторинга динамики культурного капитала организации. Личностные критерии включают в себя: уровень конвертации культурного капитала

сотрудников в культурный капитал организации; уровень глубины оснований взаимного доверия работодателей и работников. Все критерии имеют специфические особенности для работодателя и работника как субъектов и объектов доверия.

Адаптация названых критериев к специфике сферы информационной безопасности позволила впервые теоретически обосновать многокритериальную классификацию оценочных уровней доверия к кадровой безопасности информационной системы, что составляет научную новизну исследования. Теоретическая значимость работы заключается в обогащении теории информационной безопасности в части методологии оценки защищенности информации за счет включения в число объектов доверия пользователей этой информации.

Выделенные семь оценочных уровней доверия к кадровой безопасности соотносятся с семью оценочными уровнями доверия к информационным технологиям, закрепленными в международном стандарте ISO/IEC 15408-3:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components». Практическая значимость исследования состоит в возможности внесения обоснованных положений в этот стандарт для повышения результативности деятельности по обеспечению информационной безопасности.

Литература

1. Глобальное исследование утечек конфиденциальной информации в I полугодии 2017 года / Аналитический центр компании InfoWatch [Электоронный ресурс] // URL: https://www.infowatch.ru/report2017_half (дата обращения: 06.01.2018).

2. ISO / IEC 15408-3: 2008 „Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components“ [Электоронный ресурс] // URL: http://www.iso.org/iso/ru/home/store/catalogue_tc /catalogue_detail.htm?csnumber=46413 (дата обращения: 06.01.2018).

3. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – М.: Стандартинформ, 2014. –151 с.

4. Доверие и недоверие в условиях развития гражданского общества / отв. ред. А.Б. Купрейченко, И.В. Мерсияновой . – М.: Издательский дом НИУ ВШЭ, 2013. – 564 с.

5. Uzzi, B. Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness // Administrative Science Quarterly. – 1997. – Vol. 42. – No. 1. – P. 35–67.

6. Ульянов, Н.Л., Астахова, Л.В. Проблема кадровой безопасности в системе стандартов информационной безопасности Банка России / Н.Л. Ульянов, Л.В. Астахова // Вестник УрФО. Безопасность в информационной сфере. - 2014. - № 4 (14). - С. 66-70.

7. Астахова, Л.В., Ефремов, В.А., Митькин, А.И. Автоматизация многофакторной оценки кадровых уязвимостей информационной безопасности / Л.В. Астахова, В.А. Ефремов, А.И. Митькин //Вестник УрФО. Безопасность в информационной сфере.- 2014.- № 4 (14). - С. 57-61.

8. Лебедева, Н.М., Татарко, А.Н. Ценности и социальный капитал как основа социально-экономического развития // Journal of Institutional Studies (Журнал институциональных исследований) . – 2010. – Т. 2, № 1. – С.17-34

9. Косьмина, Е.А., Метелев, С.Е., Косьмин, А.Д. Культурный капитал общества в реальном материале функционирующей организации. – М.: Экономика, 2007. – 386с.

10. Астахова, Л.В. Информационная безопасность: риски, связанные с культурным капиталом персонала // НТИ. Сер.1 . – 2015– №4. – С.1-13.

11. Rosenquist, M. Prioritizing Information Security Risks with Threat Agent Risk Assessment [Электронный ресурс] // Intel Information Security – URL: http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf (дата обращения: 06.01.2018).

12. Jensen, M.C. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure / M.C. Jensen, W.H. Meckling. Harvard University Press, 2000. – 78 с.

13. Milgrom, P.R. Economics, Organization and Management. / Paul Milgrom, Jhon Roberts. Prentice-Hall, 1992. 621 с.

14. Durham, G. Measuring trust inside organisations/G. Durham, D. Hartog// Personnel Review, Vol. 35 Iss: 5, pp.557 – 588.

15. Coltri,L. Conflict diagnosis and alternative dispute resolution / L.Coltri - Upper Saddle River, N.J. : Prentice Hall, 2004.

16. Rao, S.R. Types of Trust in organizational relationships [электронный ресурс] // [Электронный ресурс] – URL: http://www.citeman.com/3621-types-of-trust-in-organizational-relationships.html#ixzz3bpKE6nYX (дата обращения: 06.01.2018).

17. Rousseau, D. M. Not So Different After All: A Cross-Discipline View of Trust / D. M Rousseau, S. Sitkin, R. S. Burt, C. Farrell Camerer, , The Academy of Management Review. - 1998; 339p.

18. Milgrom P.R. Economics, Organization and Management. / Paul Milgrom, Jhon Roberts. Prentice-Hall, 1992. 621 c.

19. Zhang R. Study on the project supervision system based on the principal-agent theory [Электронныйресурс] / Runtong Zhang, Yang Zhou, Hongnan Zhuang. Journal of Industrial Engineering and Management, 2015. 17 c. // [Электронный ресурс] – URL: http://www.jiem.org/index.php/jiem/article/view/1328 (дата обращения: 06.01.2018).

20. Бадалова, А.Г., Москвитин, К.П. Кадры риска: управление кадровыми рисками предприятия // Российское предпринимательство. - 2005. - № 7. - С. 92-98.

21. Астахова, Л.В. Доверие к безопасности информационных технологий как объект изучения будущими специалистами по защите информации // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. - 2016. - Т. 8. № 2. - С.19-23.

Reference

1. Global'noe issledovanie utechek konfidencial'noj informacii v I polugodii 2017 goda / Analiticheskij centr kompanii InfoWatch [EHlektoronnyj resurs] // URL: https://www.infowatch.ru/report2017_half (data obrashcheniya: 06.01.2018).

2. ISO / IEC 15408-3: 2008 "Information technology - Security techniques - Evaluation criteria for IT security - Part 3. Security assurance components" [EHlektoronnyj resurs] // URL: http://www.iso.org/iso/ru/home/store/catalogue_tc /catalogue_detail.htm?csnumber=46413 (data obrashcheniya: 06.01.2018).

3. GOST R ISO/MEHK 15408-3-2013 Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tekhnologij. CHast' 3. Komponenty doveriya k bezopasnosti. – M.: Standartinform, 2014. –151 s.

4. Doverie i nedoverie v usloviyah razvitiya grazhdanskogo obshchestva / otv. red. A.B. Kuprejchenko, I.V. Mersiyanovoj . – M.: Izdatel'skij dom NIU VSHEH, 2013. – 564 s.

5. Uzzi, B. Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness // Administrative Science Quarterly. – 1997. – Vol. 42. – No. 1. – P. 35–67.

6. Ul'yanov, N.L., Astahova, L.V. Problema kadrovoj bezopasnosti v sisteme standartov informacionnoj bezopasnosti Banka Rossii / N.L. Ul'yanov, L.V. Astahova // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. - 2014. - № 4 (14). - S. 66-70.

7. Astahova, L.V., Efremov, V.A., Mit'kin, A.I. Avtomatizaciya mnogofaktornoj ocenki kadrovyh uyazvimostej informacionnoj bezopasnosti / L.V. Astahova, V.A. Efremov, A.I. Mit'kin //Vestnik UrFO. Bezopasnost' v informacionnoj sfere.- 2014.- № 4 (14). - S. 57-61.

8. Lebedeva, N.M., Tatarko, A.N. Cennosti i social'nyj kapital kak osnova social'no-ehkonomicheskogo razvitiya // Journal of Institutional Studies (ZHurnal institucional'nyh issledovanij) . – 2010. – T. 2, № 1. – S.17-34

9. Kos'mina, E.A., Metelev, S.E., Kos'min, A.D. Kul'turnyj kapital obshchestva v real'nom materiale funkcioniruyushchej organizacii. – M.: EHkonomika, 2007. – 386s.

10. Astahova, L.V. Informacionnaya bezopasnost': riski, svyazannye s kul'turnym kapitalom personala // NTI. Ser.1 . – 2015– №4. – S.1-13.

11. Rosenquist, M. Prioritizing Information Security Risks with Threat Agent Risk Assessment [EHlektronnyj resurs] // Intel Information Security – URL: http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf (data obrashcheniya: 06.01.2018).

12. Jensen, M.C. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure / M.C. Jensen, W.H. Meckling. Harvard University Press, 2000. – 78 s.

13. Milgrom, P.R. Economics, Organization and Management. / Paul Milgrom, Jhon Roberts. Prentice-Hall, 1992. 621 c.

14. Durham, G. Measuring trust inside organisations/G. Durham, D. Hartog// Personnel Review, Vol. 35 Iss: 5, pp.557 – 588.

15. Coltri,L. Conflict diagnosis and alternative dispute resolution / L.Coltri - Upper Saddle River, N.J. : Prentice Hall, 2004.

16. Rao, S.R. Types of Trust in organizational relationships [ehlektronnyj resurs] // [EHlektronnyj resurs] – URL: http://www.citeman.com/3621-types-of-trust-in-organizational-relationships.html#ixzz3bpKE6nYX (data obrashcheniya: 06.01.2018).

17. Rousseau, D. M. Not So Different After All: A Cross-Discipline View of Trust / D. M Rousseau, S. Sitkin, R. S. Burt, C. Farrell Camerer, , The Academy of Management Review. - 1998; 339r.

18. Milgrom P.R. Economics, Organization and Management. / Paul Milgrom, Jhon Roberts. Prentice-Hall, 1992. 621 c.

19. Zhang R. Study on the project supervision system based on the principal-agent theory [EHlektronnyjresurs] / Runtong Zhang, Yang Zhou, Hongnan Zhuang. Journal of Industrial Engineering and Management, 2015. 17 c. // [EHlektronnyj resurs] – URL: http://www.jiem.org/index.php/jiem/article/view/1328 (data obrashcheniya: 06.01.2018).

20. Badalova, A.G., Moskvitin, K.P. Kadry riska: upravlenie kadrovymi riskami predpriyatiya // Rossijskoe predprinimatel'stvo. - 2005. - № 7. - S. 92-98.

21. Astahova, L.V. Doverie k bezopasnosti informacionnyh tekhnologij kak ob"ekt izucheniya budushchimi specialistami po zashchite informacii // Vestnik YUzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Obrazovanie. Pedagogicheskie nauki. - 2016. - T. 8. № 2. - S.19-23.

АСТАХОВА Людмила Викторовна, д.п.н., профессор, профессор кафедры защиты информации Южно-Уральского государственного университета, Челябинск, Россия. E-mail: lvastachova@mail.ru

ASTAKHOVA Lyudmila, Information Security Department, South Ural State University, Chelyabinsk, Russia. E-mail: lvastachova@mail.ru