

Ю. М. Краковский¹, К. В. Затрутина¹

¹Иркутский государственный университет путей сообщения, г. Иркутск, Россия

ВЫБОР И РАНЖИРОВАНИЕ КОМПЕТЕНЦИЙ ПЕРСОНАЛА, ОБСЛУЖИВАЮЩЕГО ИНФОРМАЦИОННУЮ СИСТЕМУ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

Аннотация. Проведены исследования по выбору и ранжированию компетенций персонала, обслуживающего информационную систему с конфиденциальной информацией. В качестве информационной системы рассматривается региональная медицинская информационная система, которая является базовой частью регионального фрагмента Единой государственной информационной системы в сфере здравоохранения. Особенностью этих систем является обработка конфиденциальной информации, включая персональные данные и врачебную тайну, связанную со здоровьем пациентов. Используя литературу по безопасности информационных систем, управлению персоналом, предложено восемь компетенций, которые затем про ранжированы по важности на основе информации выбранных экспертов. Полученные коэффициенты относительной важности рекомендуются использовать при создании рабочей программы повышения квалификации персонала, обслуживающего информационную систему.

Ключевые слова: компетенции, безопасность информационных систем, управление персоналом, экспертные методы ранжирования.

Y. M. Krakovsky¹, K. V. Zatrutina¹

¹Irkutsk State Transport University, Irkutsk, Russia

SELECTION AND RANKING OF THE COMPETENCIES OF THE SERVICE STAFF INFORMATION SYSTEM WITH CONFIDENTIAL INFORMATION

Abstract. Research was conducted on the selection and ranking of competencies of personnel serving the information system with confidential information. The regional medical information system, which is the basic part of the regional fragment of the Unified State Information System in the field of healthcare, is considered as an information system. A feature of these systems is the processing of confidential information, including personal data and medical secrets related to the health of patients. Using the literature on information system security and personnel management, eight competencies are proposed, which are then ranked by importance based on the information of selected experts. The obtained coefficients of relative importance are recommended to be used when creating a work program for improving the skills of personnel serving the information system.

Keywords: competencies, security of information systems, personnel management, expert ranking methods

Введение

В связи с тем, что в последнее время в нашей стране уделяется большое внимание «Цифровизации экономики», реализации направлений «Информационная безопасность» и «Кадры для цифровой экономики», требуется повысить квалификацию персонала, обслуживающих информационные системы, содержащих конфиденциальную информацию.

В данной работе в качестве информационной системы (ИС) рассматривается региональная медицинская информационная система, которая является базовой частью регионального фрагмента Единой государственной информационной системы в сфере здравоохранения. Особенностью этих ИС является обработка конфиденциальной информации, включая персональные данные и врачебную тайну, связанную со здоровьем пациентов.

Целью работы является создание и апробация процедуры ранжирования компетенций персонала, обслуживающего информационную систему в сфере здравоохранения.

Для реализации данной цели в работе предложено рассмотреть следующие задачи:

1) провести выбор компетенций персонала, обслуживающего ИС с конфиденциальной информацией;

2) выбрать метод ранжирования для компетенций;

3) провести ранжирования компетенций по информации экспертов.

Вопросам обработки и защиты конфиденциальной информации, включая персональные

данные, посвящено большое число нормативно-правовых документов и учебных пособий [1 - 3]. Это связано с тем, что информационные системы, обрабатывающие подобную информацию, должны содержать специальные средства ее защиты. А это, в свою очередь, предъявляет дополнительные требования компетенциям персонала, обслуживающего эту информационную систему.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» №149 [1] конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Наилучшим средством обеспечения конфиденциальности информации в электронном документообороте являются технологии симметричного шифрования. В РФ для этой технологии созданы различные национальные стандарты [4 - 6].

Компетенции – это личностные качества и способности, а также профессиональные навыки, необходимые сотруднику для успешного выполнения своих должностных обязанностей, например: умение ставить четкие цели; планирование и организация; лидерство; ориентация на результат; сбор и анализ информации; генерирование и накопление идей; навыки коммуникации; умение работать в группе; адаптивность к изменениям; личное развитие [7].

Понятие «компетенция персонала» является достаточно новым, поэтому различные авторы допускают вариации в его трактовке. Остановимся на одном из них, как на наиболее распространенном [8]: «Компетенция – это сочетание квалификации работника, т.е. его знаний, пониманий, умений и навыков с предоставленными ему полномочиями, обеспечивающими эффективную реализацию его функций».

Выбор компетенций персонала

Обоснование и выбор компетенций для сотрудников, обслуживающих информационную систему по обработке конфиденциальной информации, проведем на основании различных документов: нормативно-правовых источников; рекомендуемых компетенций образовательных программ, связанных с информационными системами и технологиями; учебной литературы, посвященной безопасности информационных систем.

В целом для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИС (зависит от определенного в итоге набора мер защиты информации в ИС);
- разработка системы защиты информации ИС (определение организационных мероприятий, выбор технических и физических средств защиты информации в том числе для реализации определенного набора мер защиты);
- внедрение системы защиты информации ИС;
- аттестация информационной системы по требованиям защиты информации (проводится лицензиатами ФСТЭК России) и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации аттестованной ИС;
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн определен приказами ФСТЭК от 18.02.2013 № 21 и от 27.03.2017 № 49. Лица, виновные в нарушении требований ФЗ [2], несут предусмотренную законодательством Российской Федерации ответственность.

Учитывая литературу по безопасности информационных систем [2, 3], методические рекомендации литературы по управлению персоналом [7, 8] и сказанное выше, предложим основные компетенции, необходимые персоналу, обслуживающего ИС применительно к сфере здравоохранения.

1. Владеет навыками и умениями контролировать и обеспечивать защищенность конфиденциальной информации (К1).

2. Способен обеспечивать целостность и доступность конфиденциальной информации (К2).
3. Владеет навыками и умениями проведения консультирования и обучения пользователей информационных технологий и систем (К3).
4. Владеет навыками и умениями антивирусной защиты конфиденциальной информации (К4).
5. Способен обеспечивать защиту носителей с конфиденциальной информацией (К5).
6. Способен обеспечивать идентификацию и аутентификацию субъектов доступа и объектов доступа (К6).
7. Владеет навыками и умениями идентифицировать уязвимости, которые могут использоваться при реализации угроз безопасности, включая специально внедренные программные закладки (К7).
8. Способен обеспечивать эффективную работу баз данных, являющихся частью обслуживаемых информационных систем, включая знания нормативных материалов по созданию требований к системе (К8).

Описание метода ранжирования выбранных компетенций

Как правило, методы ранжирования основаны на экспертной информации. Важным вопросом при обработке экспертной информации является наличие или отсутствие согласованности оценок экспертов. Мы выбрали метод простого ранжирования, основанного на рангах. Этот метод вследствие возможности проверки согласованности экспертов широко используется на практике [3, 9]. Его достоинства – относительно простой подбор экспертов и возможность проверки их однородности.

Пусть необходимо группой экспертов про ранжировать m компетенций, L – число экспертов. Эксперты для каждой компетенции проставляют ранги. При этом наименее важной компетенции ставится единица, а наиболее важной – m .

Тогда коэффициенты относительной важности (КОВ) определяются так

$$w_j = \sum_{l=1}^L r_{jl} / \sum_{j=1}^m \sum_{l=1}^L r_{jl}, \quad \sum_{j=1}^m w_j = 1, \quad (1)$$

где r_{jl} – ранг, поставленный j -ой компетенции l -ым экспертом. Если эксперт не может различить некоторые компетенции (присваивает им одинаковые ранги), то эти ранги должны быть такими, чтобы итоговая сумма рангов равнялась сумме натуральных чисел.

Однородность экспертов можно оценить коэффициентом конкордации

$$V = \frac{12S}{L^2(m^3 - m)}, \quad 0 < V < 1, \quad (2)$$

где

$$S = \sum_{j=1}^m \left(\sum_{l=1}^L r_{jl} - \frac{1}{2} L(m+1) \right)^2. \quad (3)$$

При $V \rightarrow 1$ наблюдается наилучшая согласованность мнений экспертов, а при $V \rightarrow 0$ – наихудшая. Более обосновано проверить гипотезу об однородности экспертов можно, используя специальные статистики. Например, при $m > 7$ можно использовать H -статистику

$$H = L(m-1) \cdot V, \quad (4)$$

которая имеет приближенно распределение χ^2 с $(L-1)$ степенями свободы. Если окажется, что $H > \chi^2_{кр}(L-1, p)$, то можно принять гипотезу об однородности экспертов при уровне значимости p . Критические значения для распределения χ^2 имеются в литературе по математической статистике [10].

Ранжирование компетенций персонала

Предложенное алгоритмическое обеспечение: (1) – (4), использует экспертную информацию в виде рангов, которую обеспечили специально подобранные эксперты. Этими экспертами являются сотрудники, знакомые с обслуживанием информационных систем в сфере здравоохранения. В целях сохранения их конфиденциальности они заменены идентификато-

рами: Эк1 – первый эксперт; Эк2 – второй эксперт; Эк3 – третий эксперт; Эк4 – четвертый эксперт.

Предложенные ими ранги компетенций приведены в таблице 1: НКом – сокращенные наименования компетенций, выбранные авторами; $\sum 1$ – сумма рангов по строкам у экспертов, эта сумма используется при определении КОВ (W); $\sum 2$ – сумма рангов по столбцам, она равна для всех экспертов, т.к. это сумма чисел от 1 до 8. В этой же таблице приведены КОВ (1), полученные в результате обработки рангов.

Таблица 1. Значения рангов и КОВ

НКом	Эк1	Эк2	Эк3	Эк4	$\sum 1$	W
К1	7	8	6	8	29	0,201
К2	4	5	5	4	18	0,126
К3	8	6	7	7	28	0,194
К4	3	2	4	5	14	0,097
К5	2	1	3	3	9	0,063
К6	1	3	2	2	8	0,055
К7	6	7	8	6	27	0,188
К8	5	4	1	1	11	0,076
$\sum 2$	36	36	36	36	144	1,0

Прежде чем доверять полученным КОВ, проверим гипотезу об однородности экспертов по H -статистике (4). Найдем величину S (3), $S=548$; коэффициент конкордации (2), $V=0,815$; значение H (4), $H=22,8$. Критическое значение для этой статистики при уровне значимости 0,05 равно 7,8. Так как расчетное значение (22,8) больше критического (7,8), то гипотезу об однородности экспертов можно принять. Выбор данной гипотезы означает, что КОВ (табл. 1) можно доверять.

В соответствии с КОВ компетенции по важности располагаются так:

К1, К3, К7, К2, К4, К8, К5, К6. (5)

В соответствии с (5) наиболее важными компетенциями с точки зрения экспертов являются:

К1 – Владеет навыками и умениями контролировать и обеспечивать защищенность конфиденциальной информации.

К3 – Владеет навыками и умениями проведения консультирования и обучения пользователей информационных технологий и систем.

К7 – Владеет навыками и умениями идентифицировать уязвимости, которые могут использоваться при реализации угроз безопасности, включая специально внедренные программные закладки.

Заключение

Полученные в результате обработки КОВ рекомендуется использовать при создании рабочей программы повышения квалификации персонала, обслуживающего информационную систему в сфере здравоохранения. Структура рабочей программы по долям часов должна соответствовать «весам» компетенций, которые должны реализоваться при повышении квалификации. Тем самым наиболее важным с точки зрения экспертов компетенциям будет уделено большое внимания в программе повышения квалификации. Предложенный подход можно использовать при создании программы повышения квалификации персонала, обслуживающего информационную систему различной предметной направленности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон № 149 от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» в редакции от 03.04.2020 г.
2. Федеральный закон № 152 от 27.07.2006 г. «О персональных данных» в редакции от 01.07.2020 г.

3. Краковский Ю. М. Защита информации / Ю.М. Краковский – Ростов н/Д: Феникс, 2017. – 347 с.
4. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Стандартиформ, 1994. – 25 с.
5. ГОСТ Р 34.12. – 2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартиформ, 2015. – 25 с.
6. ГОСТ Р 34.13. – 2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартиформ, 2015. – 42 с.
7. Чернятин С. В. Модель компетенций для профессионального развития менеджеров вертикально интегрированной компании / С.В. Чернятин // Кадровик. Кадровый менеджмент. – 2011. – № 6. – С. 125-131.
8. Кибанов А. Я. Управление персоналом организации / А.Я. Кибанов – М.: ИНФРА-М, 2010. – 695 с.
9. Орлов А.И. Теория принятия решений. - М.: Изд-во «Март», 2004. – 656 с.
10. Носко В.П. Эконометрика / В.П. Носко. – М: Издательский дом «Дело» РАНХиГС, 2011. – Кн.1. – 672 с.

REFERENCES

1. *Federal'nyi zakon № 149 ot 27.07.2006 g. «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» v redaktsii ot 03.04.2020 g.* [Federal Law no. 149 of 27.07.2006 "On Information, Information Technologies and Information Protection" as amended on 03.04.2020]
2. *Federal'nyi zakon № 152 ot 27.07.2006 g. «O personal'nykh dannykh» v redaktsii ot 01.07.2020 g.* [Federal Law no. 152 of 27.07.2006 "On Personal Data" as amended on 01.07.2020]
3. *Krakovsky Y. M. Zashchita informatsii* [Protection of information] Krakovsky Y.M. – Rostov-on-Don: Feniks, 2017 - 347 p.
4. *GOST 28147-89. Sistema obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya* [GOST 28147-89. Information processing system. Cryptographic protection. The algorithm cryptographic transformation.] – Moscow: Standartinform, 1994. - 25 p.
5. *GOST R 34.12. – 2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry* [GOST R 34.12. - 2015. Information technology. Cryptographic protection of information. Block ciphers] - Moscow: Standartinform, 2015. - 25 p.
6. *GOST R 34.13. – 2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Rezhimy raboty blochnykh shifrov* [GOST R 34.13. - 2015. Information technology. Cryptographic protection of information. Modes of operation of block ciphers] - Moscow: Standartinform, 2015. - 42 p.
7. Chernyatin S. V. *Model' kompetentsii dlya professional'nogo razvitiya menedzherov vertikal'no integrirovannoi kompanii* [Competence model for professional development of managers of a vertically integrated company], Chernyatin S. V., Kadrovik. Kadrovyi menedzhment. – 2011. – no. 6. – 125-131 pp.
8. Kibanov A. Y. *Upravlenie personalom organizatsii* [The management staff of the organization], Kibanov A. Y. – Moscow: INFRA-M, 2010. – 695 p.
9. Orlov A.I. *Teoriya prinyatiya reshenii* [Decision theory] - Moscow: “Mart” Publ, 2004. – 656 p.
10. Nosko V.P. *Ehkonometrika* [Econometrics], Nosko V.P. – Moscow: “Delo” RANKhIGS Publ, 2011. – book 1. – 672 p.

Информация об авторах

Краковский Юрий Мечеславович - д. т. н., профессор, профессор кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: 79149267772@yandex.ru

Затрутина Кристина Викторовна – студент магистратуры кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: kristina.zatrutina@mail.ru

Authors

Krakovsky Yuri Mecheslavovich - Doctor of Technical Sciences, Professor of the Department «Information Systems and Information Security», Irkutsk State Transport University (ISTU), Irkutsk, e-mail: 79149267772@yandex.ru

Zatrutina Kristina Victorovna - graduate student of the Department «Information Systems and Information Security», Irkutsk State Transport University (ISTU), Irkutsk, e-mail: kristina.zatrutina@mail.ru

Для цитирования

Краковский Ю.М. Выбор и ранжирование компетенций персонала, обслуживающего информационную систему с конфиденциальной информацией [Электронный ресурс] / Ю.М. Краковский, К.В. Затрутина // Молодая наука Сибири: электрон. науч. журн. – 2021. – №1(11). – Режим доступа: <http://mnv.ircups.ru/toma/111-2021>, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 14.04.2021)

For citation

Krakovsky Yu. M., Zatrutina K. V. Vybór i ranžirovanie kompetencij personala, obsluzhivayushchego informacionnyu sistemú s konfidencial'noj informaciej [Selection and ranking of the competencies of the service staff information system with confidential information]. *The electronic scientific journal "Young science of Siberia"*, 2021, no.1(11). [Accessed 14/04/2021]