6. Zin A.M., Bongsu M.S., Idrus S.M., Zulkifli M. An overview of Radio-over-Fiber network technology. *Proceedings of IEEE International Conference on Photonics*, 2010, pp. 1-3. doi: 10.1109/ICP.2010.5604429
7. Vyas A.K., Agrawal N. Radio over Fiber: Future Technology of Communication. *International Journal of Emerging Trends and technology in Computer Science*, 2012, vol. 1, no. 2, pp. 233-237.
8. Karthikeyan R., Prakasam S. A survey on Radio over Fiber (RoF) for wireless broadband access technologies. *International Journal of Computer Applications*, 2013, vol. 64, no. 12, pp. 14-19.
9. Pooja M., Saroj Sh., Manisha Bh. Advantages and limitations of radio over fiber system. *International Journal of Computer Science and Mobile Computing*, 2015, vol. 4, no. 5, pp. 506-511.
10. Reddy V., Jolly R. Radio over fiber technology (RoF) and integration of microwave and optical network for wireless access. *International Journal of Compute Applications. Proceedings of International Conference and Workshop on Emerging Trends and Technology*, 2015, pp. 9-13.
11. Capmany J., Novak D. Microwave photonics combine two worlds. *Nature*, 2007, vol. 1, pp. 319-330. doi:10.1038/nphoton.2007.89
12. Lim Ch., Yang Y., Nirmalathas A. Transport schemes for wireless technologies: transmission performance and energy efficiency. *Photonics*, 2014, vol. 1, 2014, pp. 67-83.

Received 15.11.2016

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 621.396.4

ИЕРАРХИЧЕСКАЯ ВЕРОЯТНОСТНАЯ МОДЕЛЬ МОНИТОРИНГА УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Губарева О.Ю., Осипов О.В., Пугин В.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: o.gubareva@psuti.ru

Расширение области применимости информационных систем приводит к более сложной их реализации и, как следствие, к необходимости защиты как отдельных модулей, так и системы в целом. В работе рассмотрена вероятностная модель мониторинга угрозы безопасности информационной системы в целом. Использование предлагаемой модели позволяет анализировать воздействие различных факторов и угроз на информационную систему и обеспечивать режим ее оптимальной работы. Предлагаемая методика проведения мониторинга угрозы информационной безопасности базируется на анализе информационных рисков и построении иерархической вероятностной модели угрозы.

Ключевые слова: информационная безопасность, информационная система, риск, анализ, информация, уязвимость, угроза, диагностическая система, вероятностная модель, формула Байеса, условная вероятность

Введение

Современный этап развития информатизации общества определяет новые методы обработки информации в различных областях народного хозяйства. Основным механизмом управления различными процессами является внедрение корпоративных информационных систем (ИС) различного назначения. Увеличение разнообразия и сложности ИС приводит к необходимости оценки уровня информационной безопасности (ИБ) системы в целом и обеспечения оптимального режима ее функционирования. Причем с каждым днем число и сложность угроз ИБ возрастает в геометрической прогрессии.

Ввиду значительного числа угроз ИБ ИС системы оценки рисков должны строиться по иерархическому принципу классификации угроз и уязвимостей. Одним из наиболее распространенных принципов классификации является классификация при помощи модели информационных потоков по трем основным угрозам:

– оценка ущерба ИС при нарушении целостности информации;

– оценка ущерба ИС при нарушении конфиденциальности информации;

– оценка ущерба ИС при нарушении доступности информации.

Для каждого уровня иерархии устанавливается соответствующий ему набор процедур (проверок),

обеспечивающих надежное дифференцирование рисков внутри уровня. После завершения процесса оценки рисков ИБ на очередном уровне процесс перемещается на следующий уровень, обеспечивающий дальнейшую детализацию рисков ИБ ИС.

Подобные схемы и соответствующие им системы дифференциальной оценки рисков ИБ ИС получили широкое распространение и достаточно подробно освещены в [5; 8; 10-11]. Для проведения мониторинга и анализа степени угроз ИБ в статическом режиме (на конкретный момент времени) используется методика диагностики ИБ системы. При рассмотрении мониторинга угроз (уязвимостей) информационной безопасности в режиме «онлайн» (то есть во временной области) необходимо использовать фрактальные методы анализа, так как, по мнению авторов, временной ряд, образуемый из угроз, относящихся к одному классу, будет обладать самоподобием.

В данной работе рассматривается диагностический подход к анализу информационных рисков ИС, основанный на иерархической вероятностной модели угрозы. В основе предлагаемой вероятностной модели лежит известная формула Байеса, которая вытекает из определения условной вероятности.

В литературе описано большое количество диагностических алгоритмов, основанных на вероятностном подходе, использующих формулу Байеса [1-4]:

$$P_k(e_i/q_{jk}) = \frac{P_k(e_i)P_k(q_{jk}/e_i)}{\sum_{i=0}^{S} P_k(e_i)P_k(q_{jk}/e_i)}, \quad (1)$$

где $P_k(e_i/q_{jk})$ – вероятность угрозы e_i при появлении уязвимости q_{jk}; $P_k(e_i)$ – вероятность реализации угрозы ИБ с уязвимостью e_i среди данной группы рисков ИБ; $P(q_{j_k}/e_i)$ – вероятность появления уязвимости q_{j_k} при угрозе ИБ e_i. Индекс k определяет номер проверки π_k.

Под проверкой $\pi_k = (k = 1, \dots, N)$ понимается некоторый эксперимент над информационной системой, заключающийся в подаче на него тестирующего воздействия (угрозы) и анализе ответа системы на это воздействие.

Формула (1) вполне подходит к задачам дифференциальной оценки рисков ИБ ИС: она позволяет выбрать одну из нескольких моделей оценки рисков ИБ ИС, основываясь на вычислении вероятностей различных угроз ИБ по вероятностям рисков ИБ, обнаруженных в информационной системе. По сути, формула (1) позволяет переставить местами причину и следствие, что нам как раз необходимо для при построении диагностической модели.

Вычисление вероятности появления уязвимости q_{j_k} при e_i угрозе ИБ $P(q_{j_k}/e_i)$ основано на предположении, что рассматриваемые уязвимости ИБ q_{j_k} являются статистически независимыми. Средняя вероятность получения уязвимости q_{j_k} при выполнении проверки π_k определяется следующим выражением:

$$P_k(q_{j_k}) = \sum_{i=0}^{S} P_k(q_{j_k}/e_i)P_k(e_i). \quad (2)$$

Для определения частоты встречаемости той или иной уязвимости ИБ ИС при угрозе e_i используется обширный информационный материал, полученный посредствам автоматического опроса пользователей системы для оценки рисков ИБ, выбранные случайным образом.

При построении модели делается следующее допущение: риски, имеющие низкое значение средней вероятности, не учитываются.

Для характеристики элементарной проверки π_k вводится в рассмотрение матрица условных вероятностей $[P_k(q_i/e_i)]$, структура которой приведена на рис. 1.

$$\left[P_k(q_i/e_i)\right] = \begin{array}{c|ccccc} & e_1 & & e_i & & e_s \\ q_1 & P_{11} & & P_{1i} & & P_{1s} \\ & \dots & & \dots & & \dots \\ q_{j_k} & P_{j_k,1} & & P_{j_k,i} & & P_{j_k,s} \\ & \dots & & \dots & & \dots \\ q_{f_k} & P_{f_k,1} & & P_{f_k,i} & & P_{f_k,s} \end{array}$$

Рис. 1. Матрица условных вероятностей для проверки π_k

Процедура оценки рисков информационной безопасности

Рассмотрим процедуру оценки рисков информационной безопасности на основе предложенной вероятностной модели. На основании показателя максимума средней информации $I(\pi_k)$ системой выбирается предварительно наиболее информативная проверка:

$$I(\pi_k) = H_k(e) - H_k(e/q), \text{ [бит]}, \quad (3)$$

где $H_k(e)$ – априорная энтропия, характеризующая состояние системы для проведения аудита ИБ ИС после завершения k-ой проверки; $H_k(e/q)$ – средняя апостериорная энтропия состояния после условного проведения проверки π_k.

Априорная энтропия до начала проверки π_k вычисляется по формуле:

$$H_k(e) = -\sum_{j=0}^{S} P_k(e_i) log_2[P_k(e_i)]. \quad (4)$$

Энтропия после условного проведения проверки π_k вычисляется по формуле:

$$H_k(e/q) = -\sum_{j_k=0}^{f_k} P_k(q_{j_k}) H_k(e/q_{j_k}), \quad (5)$$

где $H_k(e/q)$ – условная энтропия, показывающая изменения неопределенности состояния рисков ИБ ИС после завершения проверки π_k исходом q_j.

Сначала производится единичное испытание: выдается вопрос и возможные варианты ответов. Ответ респондента с помощью специальной процедуры записывается в исход q_j.

Далее из матрицы условной вероятности выбирается строка условных вероятностей $P(q_j/e_i) \ldots P(q_j/e_s)$, которая соответствует полученной уязвимости ИБ. Затем по формуле Байеса (1) для конкурирующих гипотез рассчитывается новое распределение вероятностей $P_k(e_i/q_{jk})$ – возможного ущерба, который будет нанесен ИС в целом после реализации угрозы ИБ ИС. Проведенная проверка исключается из списка. Цикл повторяется до тех пор, пока значение вероятности одной из угроз не превысит заданного порогового уровня или не исчерпается весь список проверок уязвимостей. По результатам проверок делается вывод о наиболее вероятном ущербе, который может быть нанесен ИС в целом после реализации угрозы. Алгоритм оценки рисков ИБ представлен на рис. 2.

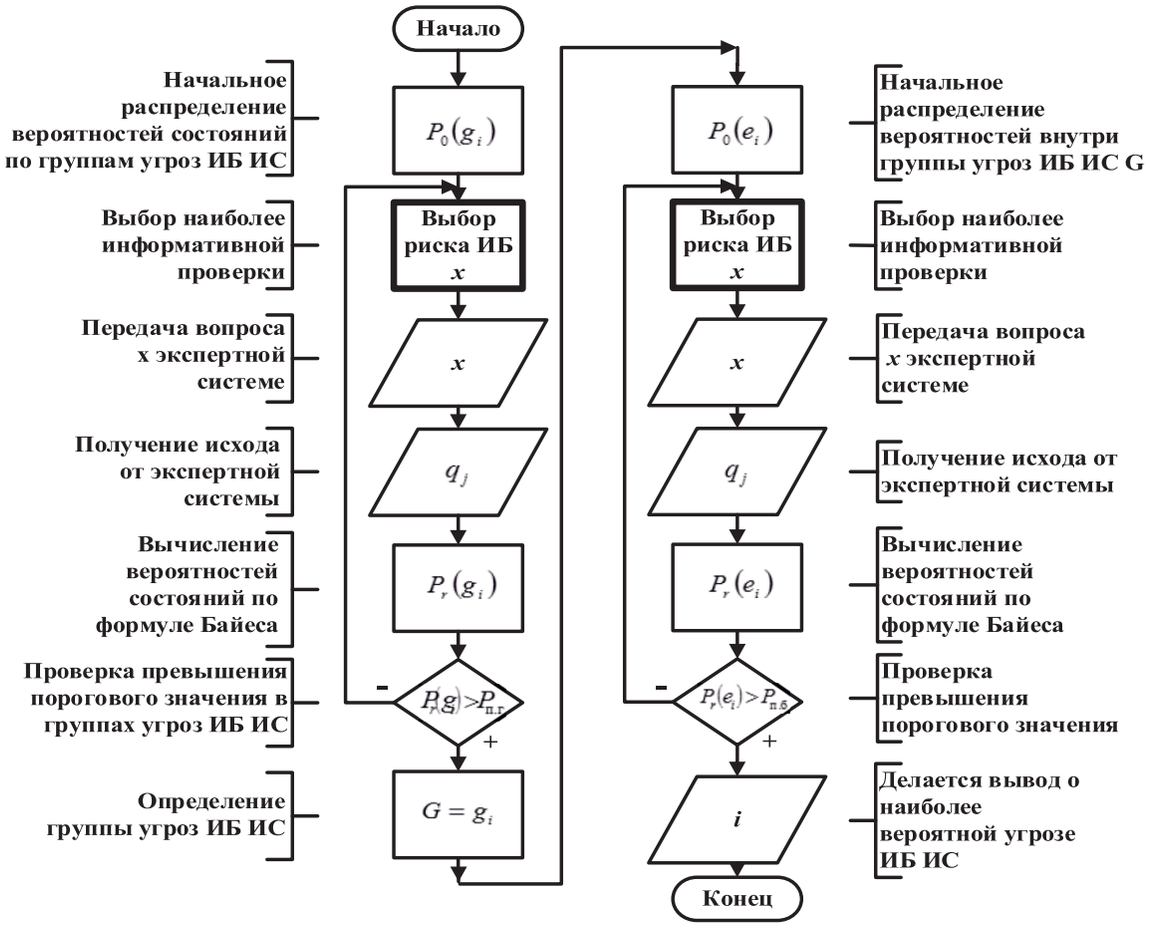

Рис. 2. Алгоритм оценки рисков информационной безопасности

Подготовка информации

Подготовка исходной информации для введения ее в базу знаний системы является наиболее трудоемким процессом, требующим от эксперта детальных знаний ИБ ИС или конкретных признаков, характеризующих каждую из угроз [6-7; 9; 12-13].

Для разработанных систем оценки рисков ИБ ИС применяется следующий алгоритм подготовки информации:

1. Процесс подготовки информации начинается с задания списков диагностируемых угроз по каждому из объектов (модулей) ИБ ИС.

2. Для каждой из угроз по выбранному объекту (модулю) ИБ ИС составляется краткое описание характерных признаков данной угрозы.

3. На основании кратких описаний для каждой угрозы составляется список характерных проверок. Условные вероятности исходов проверок являются экспертными оценками. В случае привлечения нескольких экспертов указываются средние значения условных вероятностей. На рис. 3 показан алгоритм выбора наиболее информативной уязвимости ИБ ИС.

4. По всем типам угроз данных объектов ИБ ИС составляется сводный перечень проверок с указанием наименований исходов каждой из проверок и условных вероятностей получения каждого исхода. Необходимо обратить внимание на то, чтобы в списке отсутствовали проверки, имеющие одинаковое назначение, но различные наименования.

5. Для каждой проверки из сводного перечня составляется матрица условных вероятностей (см. рис. 2) исходов всех рассматриваемых угроз данных объектов ИБ ИС. В элементы указанной матрицы записываются условные вероятности получения исхода данной проверки при условии конкретной угрозы.

Для того чтобы перечень угроз представлял полную систему (то есть сумма всех вероятностей была равна единице), вводятся два дополнительных состояния: одно из которых соответствует отсутствию угроз, а второе – наличию в системе ИБ «новой» угрозы, не входящей в общий перечень.

Вероятности исходов по первому состоянию устанавливаются экспертным путем. Распределение условных вероятностей исходов по состоянию «новой угрозы» следует считать равномерным, то есть предполагается, что все исходы являются равновероятными.

Если проверка не характерна для данной угрозы, то распределение условных вероятностей

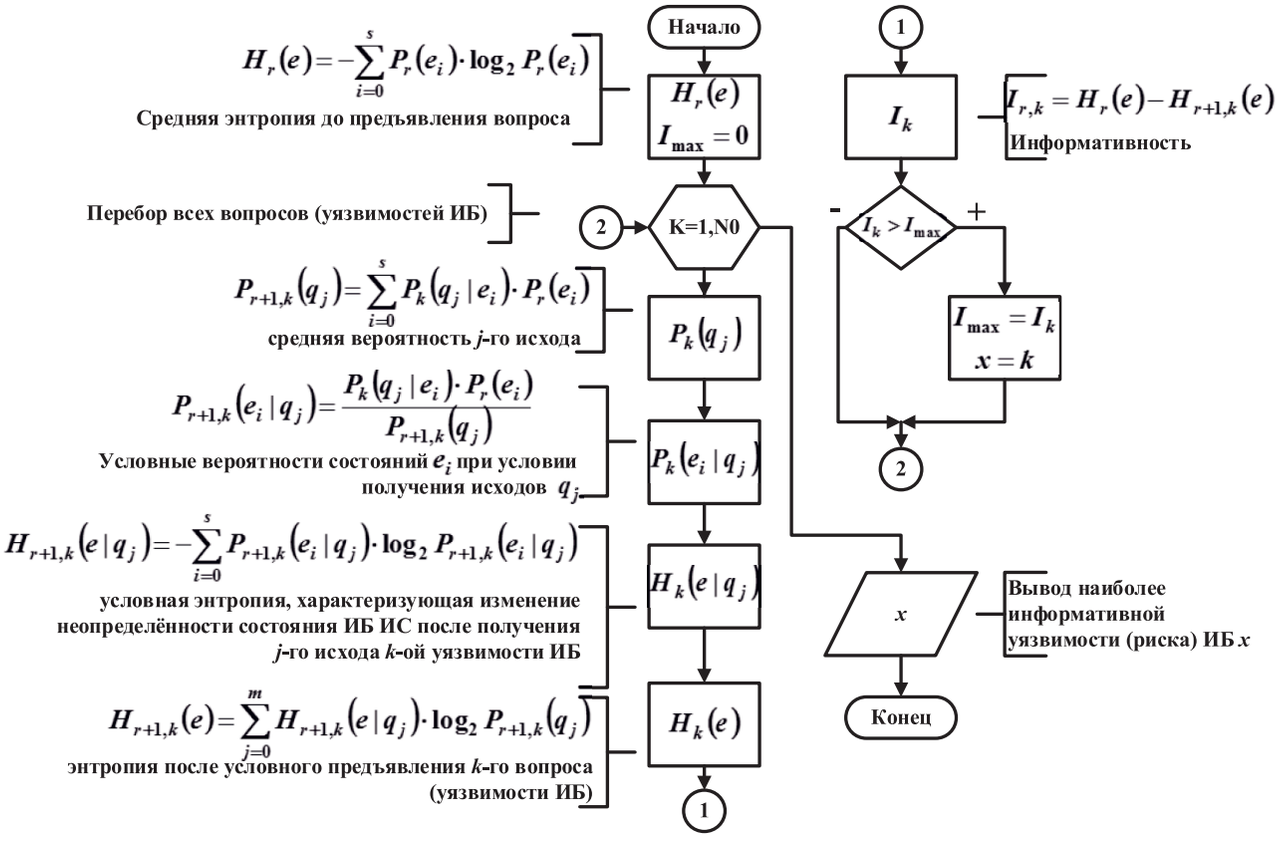

Рис. 3. Алгоритм выбора наиболее информативной уязвимости ИБ ИС

исходов, соответствующее этой угрозе также следует считать равновероятным.

6. Полученные таким образом матрицы проверок представляют исходную информацию, которая вводится в базу знаний системы и обеспечивает ее функционирование.

Выводы

1. Оценка рисков информационной безопасности носит вероятностный характер. Действительная угроза ИБ ИС из группы угроз (рисков) ИБ может быть определена только лишь с некоторой степенью вероятности.

2. Процесс оценки рисков ИБ может быть представлен в виде последовательности элементарных проверок, каждая из которых характеризуется матрицей условной вероятности. Значения элементов определяются законами распределения контролируемых параметров.

3. Предложен алгоритм, позволяющий из множества доступных элементарных проверок выбрать такую последовательность проверок, которая обеспечивает наибольшую информационную производительность процесса оценки рисков ИБ ИС.

4. Предложенная вероятностная модель обеспечивает возможность реализации распределенных систем оценки рисков ИБ, используемых в компьютерных сетях, для каждого из уровней иерархии классификации угроз ИБ ИС.

5. Для развития результатов представленной работы при рассмотрении мониторинга угроз (уязвимостей) информационной безопасности в режиме реального времени необходимо использовать фрактальные методы анализа.

Литература

1. Лихтциндер Б.Я., Аверьянов С.В., Пугин В.В., Шигаев В.В. Использование вероятностных методов оценки знаний при разработке тестирующих модулей распределенных тренинг-систем // ИКТ. Т. 1, №3, 2003. – С. 40-45.
2. Brand E., Gerritsen R. Naive-Bayes and Nearest Neighbor // DBMS. No7, 1998. – P. 131-165.
3. Friedman N., Geiger D., Goldszmidt M. e.a. Bayesian Network // Machine Learning. No 29, 1997. – P. 131-165.
4. Heckerman D. Bayesian Networks for Data Mining // Data Mining and Knowledge Discovery. No 1, 1997. – P. 79-119.
5. Куканова Н. Методика оценки риска ГРИФ 2006 из состава Digital Security Office6 // URL: https://dsec.ru/ipm-research-center article/ (д.о. 22.10.2016)/
6. Сердюк В. Аудит информационной безопасности. BYTE Россия, №4 (92), 2006 // URL: http://www.bytemag.ru/articles/detail. php?ID=6781 (д.о. 22.10.2016)/
7. Петренко С.А. Возможная методика построения системы информационной безопасности предприятия. Security.meganet.md // URL: http://bre.ru/ security/13985.html (д.о. 22.10.2016).
8. Software Engineering Institute Carnegie Mellon. OCTAVE // URL: www.cert.org/octave (д.о. 22.10.2016).
9. Siemens. The total information security toolkit // URL: http://www.cramm.com (д.о. 22.10.2016).
10. Пугин В.В., Губарева О.Ю. Методика Risk Watch для анализа рисков в сфере информационной безопасности // Материалы XIX РНТК ПГУТИ, 2012. – С. 53.
11. Пугин В.В., Губарева О.Ю. Методика FRAP для анализа рисков в сфере информационной безопасности. // Материалы XIX РНТК ПГУТИ, 2012. – С. 50.
12. Harshna, Navneet Kaur. Fuzzy Data Mining Based Intrusion Detection System Using Genetic Algorithm // International Journal of Advanced Research in Computer and Communication Engineering. Vol. 3, No. 1, 2014. – P. 5021-5028.
13. Anoop Singhal, Ximming Ou. Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs // NIST Interagency Report 778. National Institute of Standards and Technology, Gaithersburg, Maryland, 2011. – 23 p.

Получено 02.11.2016

Губарева Ольга Юрьевна, зам. начальника Научно-исследовательского отдела Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-927-732-12-11. E-mail: o.gubareva@psuti.ru

Осипов Олег Владимирович, д.ф.-м.н., доцент, Проректор по информатизации и образовательным технологиям ПГУТИ. Тел. 8-917-941-10-73. E-mail: o.osipov@psuti.ru

Пугин Владимир Владимирович, к.т.н., доцент, декан Факультета заочного обучения ПГУТИ. Тел. 8-927-203-30-00. E-mail: pugin@psati.ru

HIERARCHICAL STOCHASTIC MODEL FOR MONITORING OF TREAT TO INFORMATION SECURITY OF INFORMATION SYSTEM

Gubareva O.Yu., Osipov O.V., Pugin V.V.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: o.gubareva@psuti.ru

Nowadays modern information systems solve various problems concerned with automation of banks, insurance and trading company activities, financial exchanges, supervisory control and data acquisition applications etc. They become more complex due to widening of their applicability that requires protection for both loose units or modules and whole system. Therefore the problems of corporate information resources security providing take on a dimension during all steps of system design and maintenance. This work considers a stochastic model for monitoring of treat to information security of the whole information system. Proposed model provides analysis of various factors and threats influence on information system and its optimum operation mode under them. This developed technique is based on analysis of information security risks and designing of threat hierarchical stochastic model. We utilize the algorithm of directed search of information security risks, which performs security risk choice by maximal information capacity criterion. It provides decreasing of analyzing threats and therefore transmitted data capacity.

Keywords: information security, information system, risk, analysis, information, vulnerability, threat, diagnostic system, stochastic model, Bayesian formula, conditional probability

DOI: 10.18469/ikt.2016.14.4.12

Gubareva Olga Yurevna, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy, Samara, 443010, Russian Federation; Deputy Head of the Science and Research Department, assistant of the Department of Multiservice Networks and Information Security. Tel.: +79277321211. E-mail: o.gubareva@psuti.ru

Osipov Oleg Vladimirovich, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy, Samara, 443010, Russian Federation; Vice-rector on Informatization and Educational Technologies, Professor of the Department of Electrodynamics and Antennas; Doctor of Physical and Mathematical Sciences, Associate Professor. Tel.: +79179411073. E-mail: o.osipov@psuti.ru

Pugin Vladimir Vladimirovich, Povolzhskiy State University of Telecommunications and Informatics, 23 L. Tolstoy, Samara, 443010, Russian Federation; Dean of the Faculty of Distance Learning, Associate Professor of the Department of Multiservice Networks and Information Security, PhD in Technical Science, Associate Professor. Tel.: +79272033000. E-mail: pugin@psati.ru

References

1. Lihtcinder B.Ja., Aver'janov S.V., Pugin V.V., Shigaev V.V. Ispol'zovanie verojatnostnyh metodov ocenki znanij pri razrabotke testirujushhih modulej raspredelennyh trening-sistem [Using probabilistic knowledge assessment methods in the development of test modules distributed training systems].*Infokommunikacionnye Tehnologii*, 2003, vol. 1, no. 3, pp. 40-45.
2. Brand, E. Naive-Bayes and Nearest Neighbor. E. Brand, R. Gerritsen. DBMS, 1998, no. 7, pp. 131-165.
3. Friedman N., Geiger D., Goldszmidt M. e.a. Bayesian Network. *Machine Learning*, 1997, no. 29, pp. 131-165.
4. Heckerman D. Bayesian Networks for Data Mining. *Data Mining and Knowledge Discovery*, 1997, no. 1, pp. 79-119.
5. Kukanova N. *Metodika ocenki riska GRIF 2006 iz sostava Digital Security Office 6*. [Technique of risk assessment of GRIF of 2006 from structure of Digital Security Office 6] Available at: https://dsec.ru/ipm-research-center/article/risk_assessment_method_vulture_2006_from_the_composition_of_the_digital_security_office/?sphrase_id=136893 (accessed 22.10.2016).
6. Serdjuk V. Audit informacionnoj bezopasnosti. [Information security audit]. *BYTE Rossija*, 2006, vol. 92, no. 4. Available at: http://www.bytemag.ru/articles/detail.php?ID=6781 (accessed 22.10.2016).

7. Petrenko S.A. *Vozmozhnaja metodika postroenija sistemy informacionnoj bezopasnosti predprijatija* [Possible technique of creation of an information security system of the enterprise]. Security.meganet.md. Available at: http://bre.ru/security/13985.html (accessed 22.10.2016).
8. Software Engineering Institute Carnegie Mellon. OCTAVE. Available at: www.cert.org/octave (accessed 22.10.2016).
9. Siemens. The total information security toolkit. Available at: http://www.cramm.com (accessed 22.10.2016).
10. Pugin V.V., Gubareva O.Ju. Metodika Risk Watch dlja analiza riskov v sfere informacionnoj bezopasnosti [Risk Watch technique for risk analysis in the field of information security]. *Materialy XIX Rossijskoj nauchnoj konferencii professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov*, 2012, no. 19, pp. 53.
11. Pugin V.V., Gubareva O.Ju. Metodika FRAP dlja analiza riskov v sfere informacionnoj bezopasnosti. [Technique of FRAP for risk analysis in the field of information security]. *Materialy XIX Rossijskoj nauchnoj konferencii professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov*, 2012, no. 19, pp. 50.
12. Harshna, Navneet Kaur. Fuzzy Data Mining Based Intrusion Detection System Using Genetic Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering*, 2014, vol. 3, no. 1, pp. 5021-5028.
13. Singhal, A. Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. Anoop Singhal, Ximming Ou. *NIST Interagency Report 778*, National Institute of Standards and Technology, 2011, 23 p.

Received 02.11.2016

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 004.7

СОВРЕМЕННЫЕ ПРИНЦИПЫ РАБОТЫ СИСТЕМЫ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

Лабанкова Е.П.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: e.labankova@mail.ru

Определены принципы улучшения процессов управления персоналом путем применения информационных систем Oracle с отслеживанием ключевых показателей эффективности. Проведен анализ работы систем управления персоналом, составлен алгоритм расчета ключевых показателей. Представленный подход исключает двойное введение данных в систему, что ведет к повышению эффективности работы сотрудников при более высоком уровне безопасности и конфиденциальности персональных данных. Анализ полученных результатов позволяет скорректировать график предоставления отчетной документации и предусмотреть внедрение временных ресурсов на этапы наибольшей загрузки сотрудников.

Ключевые слова: управление персоналом, системы кадрового администрирования, информационные системы управления персоналом, оптимизация процесса, ключевые показатели эффективности, Fusion, Oracle

Введение

Большинству предприятий в кризисный период приходится закрывать набор новых сотрудников, а также проводить масштабные сокращения, поскольку экономически неблагоприятная ситуация не способствует развитию бизнеса. В то же время новые специалисты бывают необходимы именно в такие тяжелые моменты. Поэтому существует множество аспектов, призванных помочь предприятию сохранить накопленных специалистов, а также пополнить резервы новыми силами.

Постановка задачи

Целью проводимого исследования является изучение инструментов, способствующих улучшению процесса управления персоналом. Одним из них является оптимизация и пересмотр существующих процессов с целью автоматизации и внедрения единого стандарта работы всех филиалов предприятия. Немаловажную роль играет квалификация самих специалистов кадрового администрирования – так как именно они отвечают за ключевые аспекты жизни предприятия: отбор специалистов, адаптацию