УДК 004.056:004.413.4

МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОЙ ЭКОНОМИКИ

Л.М. ЛЫНЬКОВ, Т.Н. БЕЛЯЦКАЯ, В.С. КНЯЗЬКОВА

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 8 февраля 2017

Аннотация. Приведены результаты анализа рисков информационной безопасности электронных виртуальных взаимосвязанных сообществ (е-кластеров), рассмотрен алгоритм минимизации рисков и контроля за формированием и динамическим изменением угроз информационной безопасности. Данный алгоритм лежит в основе методики оценки рисков информационной безопасности е-кластера.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, электронная экономика, е-кластер.

Abstract. The results of information security risks analyses in electronic virtual interconnected associations (e-clusters) are presented. Algorithm of risk minimization and control on formation and dynamic changing of information security alerts is examined. This algorithm is a basis of methodology of risk evaluation in e-clusters' information security.

Keywords: information security, information security threats, e-economy, e-cluster.

Doklady BGUIR. 2017, Vol. 104, No. 2, pp. 69-76
Methodology of risks assessment of information security evaluation in e-economy systems
L.M. Lynkov, T.N. Beliatskaya, V.S. Knyazkova

Введение

Электронная экономическая система может быть определена как совокупность распределенных и автоматизированных (в разной степени) социотехнических подсистем, взаимосвязанных инфокоммуникациями, экономическими законами и законами управления [1]. В ней все большую актуальность приобретают проблемы информационной безопасности (ИБ). Ряд исследований подтвердили предположение о том, что финансовые убытки, возникающие в результате нарушений системы ИБ, в значительной степени зависят от формы и размера организации. В крупных компаниях обычно более эффективно внедрены бизнес-процессы по управлению системами ИБ, в то время как организациям малого бизнеса сложно организовать комплексную систему защиты информации главным образом из-за ограниченности ресурсов. Одним из решений данной проблемы может быть формирование целевого объединения организаций в форме электронных виртуальных экономически взаимосвязанных сообществ (е-кластеров). Такие сообщества могут создаваться в различных отраслях экономики любыми хозяйствующими субъектами, функционирующими в одной технологической цепочке, использующими сеть интернет в своей хозяйственной деятельности.

Отличительной особенностью организации системы ИБ в е-кластере является необходимость обеспечения удаленного доступа различных пользователей (участников е-кластера) к информации, программному обеспечению и даже аппаратным мощностям. Подобный подход требует повышенного внимания к безопасности, разграничению прав, изолированию данных и программных продуктов, а также к балансировке нагрузки на

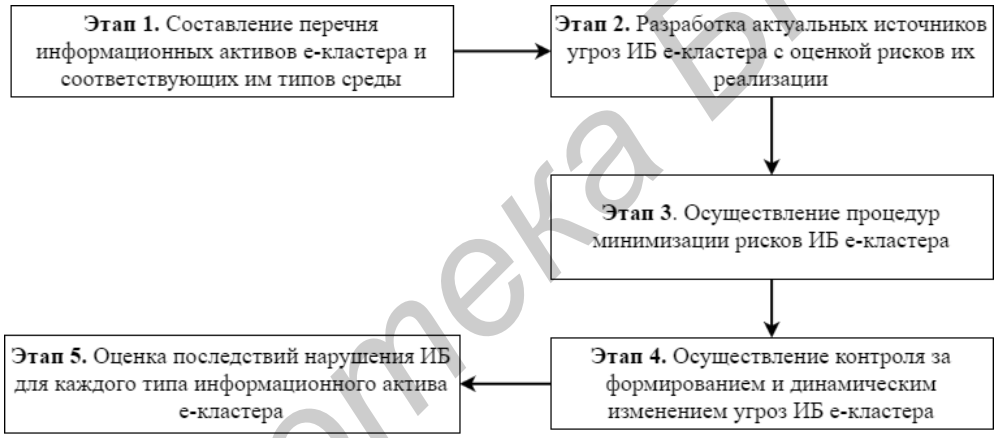
аппаратную часть. В связи с этим предъявляется ряд требований к обеспечению приемлемых уровней риска ИБ, которые будут зависеть от ценности информационного актива.

Таким образом, процессы функционирования организаций е-кластера формируют актуальную проблему формирования методологического подхода для обеспечения ИБ, в частности – снижения рисков ИБ в кластерах электронного бизнеса. Указанная задача может быть решена через выявление, анализ и оценку рисков, снижение значения рисков до приемлемого для организации уровня, а также внедрения необходимых механизмов обеспечения системы ИБ непосредственно для тех процессов и систем, для которых они необходимы – то есть через реализацию методики оценки рисков ИБ е-кластера.

Методика оценки рисков информационной безопасности е-кластеров

Под риском нарушения ИБ будем понимать возможность утраты свойств ИБ информационных активов в результате реализации угроз ИБ, вследствие чего е-кластеру может быть нанесен ущерб; при этом угрозы ИБ реализуются их источниками, которые могут воздействовать на объекты среды информационных активов е-кластера [2, 3].

Основная задача, решаемая в системе управления рисками е-кластера, заключается в том, чтобы оценить риск ИБ е-кластера с целью принятия эффективных и экономически обоснованных мер по защите информации. На рисунке приведен алгоритм реализации оценки рисков ИБ е-кластеров.



Алгоритм реализации оценки рисков ИБ е-кластеров

Этап 1. Составление перечня информационных активов е-кластера и соответствующих им типов среды. Основная задача, стоящая на данном этапе – выявление используемых активов. Под активами понимаются материальные и нематериальные ресурсы организации, способные приносить прибыль и увеличивать доход в ближайшем будущем или через некоторое время. Обычно выделяют следующие типы активов [4]: информация/данные; аппаратные средства; программное обеспечение, включая прикладные программы; оборудование для обеспечения связи; программно-аппаратные средства; документы; продукция и услуги; конфиденциальность и доверие при оказании услуг; оборудование, обеспечивающее необходимые условия работы; персонал организации; престиж (имидж) организации. Для каждого типа информационного актива далее определяется перечень свойств ИБ, поддержание которых необходимо обеспечить для бесперебойного функционирования организации (конфиденциальность, целостность, доступность).

Далее для каждого из выделенных типов информационных активов необходимо составить перечень типов объектов среды. К ним относятся: линии связи и сети передачи данных; сетевые программные и аппаратные средства; файлы данных, базы данных, хранилища данных; носители информации; программно-технические компоненты автоматизированных систем; помещения, здания, сооружения; платежные и информационные технологические процессы; бизнес-процессы организаций, входящих в е-кластер.

Этап 2. Разработка актуальных источников угроз ИБ е-кластера с оценкой рисков их реализации. Для каждого типа объекта среды и информационного актива формируется

перечень актуальных источников угроз, воздействие которых может привести к потере значимых свойств ИБ информационных активов. Перечень актуальных источников угроз формируется на основе модели угроз.

Типичными для всех уровней интеграции электронного бизнеса (ЭБ) будут следующие угрозы [5]:

– угроза потери целостности информации о бизнес-процессах и бизнес-операциях;

– угрозы вирусной атаки и подверженность мошенничеству со стороны потребителей и иных лиц посредством несанкционированного доступа к информации;

несоблюдение требований нормативно-правового регулирования финансово-хозяйственной деятельности и, в частности, ЭБ из-за отсутствия четко выработанной законодательной системы в этой сфере;

– сбой или отказ систем и элементов информационных инфраструктур.

Этап 3. Алгоритм минимизации рисков информационной безопасности е-кластера. В соответствии с существующими международными и национальными стандартами в области управления риска ИБ, допускается использование как количественных, так и качественных методов оценки рисков. Под задачей снижения риска обычно понимаются действия, предпринятые для уменьшения вероятности и/или негативных последствий риска.

Итак, стоит задача по минимизацию рисков ИБ в е-кластере. Мы предлагаем рассмотреть ее как решение экстремальной задачи на основе линейного программирования (ЛП) [6].

Линейное программирование представляет собой набор переменных $x = (x_1, x_2, \ldots x_n)$ и функции этих переменных $f(x) = f(x_1, x_2, \ldots x_n)$, которая называется целевой функцией. Таким образом, необходимо найти экстремум (максимум или минимум) целевой функции $f(x)$ при условии, что переменные x принадлежат некоторой области Q.

Рассмотрение задачи ЛП предполагает, что:

– функция $f(x)$ является линейной функцией переменных $x_1, x_2, \ldots x_n$;

– область Q определяется системой линейных равенств или неравенств.

Для оценки рисков ИБ в е-кластере представим формально задачу следующим образом. Пусть в нем может находиться информация различной степени конфиденциальности $c = 1, 2, \ldots, M$, где M – количество степеней конфиденциальности информации. Согласно мандатной модели разграничения доступа при обработке информации c-й степени конфиденциальности на ресурсе k-го уровня защищенности должно выполняться следующее требование: $c \le k$. Пусть известны затраты S_k на обеспечение функционирования единицы информационного ресурса различных уровней защищенности $S_1, S_2, \ldots, S_M$ и заданы стоимости обработки единицы информации E_c различной степени конфиденциальности $E_1, E_2, \ldots, E_M$. Известен также поток заявок $I = \{I_1, I_2, \ldots, I_c\}$ на обработку информации различной степени конфиденциальности.

Обычно риск (R) находят как произведение вероятности и ущерба от реализации угрозы:

$$R = \sum_i P_i S_i, \qquad (1)$$

где P_i – вероятность успешной реализации i-й угрозы, S_i – оценка ущерба от реализации i-й угрозы; $i = 1 \ldots n$ – количество вероятных угроз.

Рассмотрим систему оценки риска ИБ е-кластера при наличии одной угрозы. Очевидно, что сумма ущерба от реализации угрозы ИБ Si будет варьироваться в зависимости от степени конфиденциальности информации. Мы можем построить матрицу рисков r, зная величины ущерба E в зависимости от c-й степени конфиденциальности информации, а также вероятности реализации угроз ИБ применительно к ресурсу k-го уровня защищенности:

$$r = \begin{matrix} r_{11} & \ldots & r_{1s} \\ \vdots & \ddots & \vdots \\ r_{k1} & \ldots & r_{ks} \end{matrix}, \qquad (2)$$

где r_{sk} – риск ИБ при воздействии угрозы на ресурс i-го класса, обрабатывающий информацию j-й степени конфиденциальности.

Найдем число единиц информационных ресурсов каждого уровня x_k, которое требуется для того, чтобы при воздействии i-й угрозы риски ИБ были минимальны. Принимая во внимание требование (1), запишем целевую функцию следующим образом:

$x_1r_{11} + x_2r_{21} + x_2r_{22} + x_3r_{31} + x_3r_{32} + x_3r_{33} + \ldots + x_Mr_{MM} \rightarrow \min.$

При этом системе ограничений необходимо обеспечить обслуживания всего потока заявок: $\sum_i x_i I_i^d \geq I.$ Кроме того, следует учесть параметр экономической рентабельности обеспечения информационной безопасности е-кластера: $\sum_i \sum_j x_i C_j^0 > \sum_i x_i C_i^k$.

Таким образом, для степени конфиденциальности $c = i$, при обработке на ресурсе уровня $k = j$ ($j > i$), стоимость обработки должна быть равной C_i^0. Отметим, что система ограничений должна быть дополнена требованиями целостности и не отрицательности величин, исходя из их физического смысла.

Основной особенностью информационной системы е-кластера является «распределенность» ресурсов. Это означает наличие в нем относительно большого числа разнотипных узлов, что предоставляет возможность создания механизма для статистического «накопления» знаний об угрозах, уязвимостях и успешности их устранения путем сопоставления оценки уязвимости k-го узла сети n-го типа с аналогичными ресурсами сети при воздействии по нему i-й угрозы по j-му каналу несанкционированной передачи информации.

Предположим, что в составе распределенной автоматизированной информационной системы некоего е-кластера имеются ресурсы различной степени защищенности (в зависимости от системы защиты информации – СЗИ, реализованной на данном ресурсе):

1-я группа (A) – ресурсы с низким уровнем защищенности;

2-я группа (B) – ресурсы с высоким уровнем защищенности;

3-я группа (C) – защищенные ресурсы.

Затраты в денежном выражении на содержание единицы ресурса n-ой группы: $A = 2, B = 5, C = 10$ условных единиц. Пусть в рассматриваемой системе обрабатывается информация различных категорий конфиденциальности l_c ($c = 1, 2, 3$): l_1 – открытая информация, l_2 – конфиденциальная информация, l_3 – критически важная информация.

Согласно неравенству (1), информация категории l_1 обрабатывается на ресурсах любой группы, информация категории l_2 может обрабатываться на ресурсах групп B и C. Информация категории l_3 обрабатывается только на ресурсах группы C. Затраты на обработку единицы информации c-ой степени конфиденциальности составляют $l_1 = 3$, $l_2 = 6$, $l_3 = 12$ условных единиц.

Масштабирование ресурсов, требуемых для обработки информации c-ой степени конфиденциальности, осуществляется при помощи заявок Z. Предположим, что поток заявок составляет не менее: $Z_1 = 250$; $Z_2 = 100$; $Z_3 = 50$ единиц.

Пусть из общей статистики угроз вида Y известна вероятность реализации угрозы P_i для каждого типа ресурсов P_A, P_B и P_C. Заметим, что P_i реализации угрозы зависит от уровня защищенности ресурса, но не зависит от степени конфиденциальности информации c, обрабатываемой на ресурсе. Составим матрицу рисков (1). Пусть значения вероятности P_i и уровня ущерба S_c^y для различных групп ресурсов и степеней конфиденциальности защищаемой информации: $P_A = 0{,}8$; $P_B = 0{,}6$; $P_C = 0{,}2$ и $S_1^y = 3$; $S_2^y = 6$; $S_3^y = 12$. Тогда элементы матрицы рисков r_{is} будут иметь значения, представленные в таблице.

Матрица рисков

Тип ресурса	Открытая информация (l_1)	Конфиденциальная информация (l_2)	Критическая информация (l_3)
Ресурс группы A	2,4	4,8	9,6
Ресурс группы B	1,8	3,6	7,2
Ресурс группы C	0,6	1,2	2,4

Проведем расчет количества емкости заявок Z_n. На ресурсах группы A могут обрабатываться категории информации $Z_1 = 250$; на ресурсах группы B обрабатываются заявки

Z_1 и Z_2 = 350 и на ресурсах группы *C* могут обрабатываться только заявки категории Z_3 = 50. Общее количество заявок Z_n составляет 400. Решение задачи симплекс-методом дало следующий результат: количество единиц ресурса группы *A* = 80 единиц; для группы *B* = 120 единиц; для группы *C* = 200 единиц.

Таким образом, мы получили количественные оценки состава ресурсов е-кластера различной степени защищенности. Данный состав будет обеспечивать экономически эффективную обработку потока заявок на доступ к информации различной степени конфиденциальности.

Этап 4. Осуществление контроля за формированием и динамическим изменением угроз ИБ е-кластера является одним из определяющих факторов обеспечения бесперебойного функционирования организаций ЭБ.

Для оценки угроз ИБ е-кластера в качестве методологической базы могут служить так называемые интеллектуальные методы анализа данных. Наиболее распространенным из них является байесовский подход, который предоставляет ряд преимуществ [6]: возможность получения апостериорной оценки вероятности инцидента; возможность отслеживания поступления новых данных; выявление зависимость между факторами, влияющими на ИБ; логическое объяснение своих выводов, физическая интерпретация и изменение структуры отношений между значениями задачи.

Предположим, что в состав информационной системы некоего е-кластера входят ресурсы различного уровня (класса) защищенности – «уровень А», «уровень В» и «уровень С». Стоит задача определить степень защищенности ресурсов исследуемой информационной системы по вышеуказанным группам от некоторой угрозы *Y* .

Таким образом, при анализе конкретного ресурса имеются три гипотезы α_i ее принадлежности *n*-й группе, *n* = 1, 2, 3. Пусть из общей статистики воздействия угроз вида *Y* на информационные ресурсы известно, что 60 % ресурсов оказались защищенными, 25 % ресурсов имеют высокую и 15 % – низкую защищенность. Используя эти данные, можно определить априорные вероятности гипотез $P(\alpha_1) = 0{,}6$; $P(\alpha_2) = 0{,}25$; $P(\alpha_3) = 0{,}15$.

В байесовский подход к оценке угроз информационной безопасности включим три показателя защищенности системы: способность системы защиты информации (СЗИ) обеспечить конфиденциальность информации при воздействии угрозы *Y* (y_1), способность СЗИ обеспечить целостность информации (y_2) и способность СЗИ обеспечить доступность информации (y_3). Предположим, что из анализа угроз такого типа известно, что при воздействии на ресурсы 1-й группы конфиденциальность обеспечивалась в 65 % случаев, при воздействии на ресурсы 2-й группы – в 75 % случаев, на ресурсы 3-й группы – в 20 % случаев. Отсюда можно записать условные вероятности $P(y_1/\alpha_1) = 0{,}65$; $P(y_1/\alpha_2) = 0{,}75$; $P(y_1/\alpha_3) = 0{,}2$. Также известно, что при воздействии угрозы *Y* имеющиеся СЗИ ресурсов 1-й группы позволили обеспечить целостность информации в 75 % случаев. Для СЗИ 2-й и 3-й группы защищенности такие показатели равны соответственно 85 % и 5 %. Тогда можно записать условные вероятности $P(y_2/\alpha_1) = 0{,}75$; $P(y_2/\alpha_2) = 0{,}85$; $P(y_2/\alpha_3) = 0{,}05$.

Далее предположим, что при воздействии угрозы *Y* имеющиеся СЗИ ресурсов 1-й группы позволили обеспечить защищенность информации в 90 % случаев, 2-й группы 80 % и 3-й группы – 10 %. Тогда можно записать условные вероятности $P(y_3/\alpha_1) = 0{,}9$; $P(y_3/\alpha_2) = 0{,}8$; $P(y_3/\alpha_3) = 0{,}1$. Предположим, что достоверно выявлено воздействие угрозы рассматриваемого типа на исследуемый или аналогичный ресурс, оснащенный одинаковыми СЗИ. При этом нарушения конфиденциальности информации, хранимой на атакованном ресурсе, не произошло. Учитывая показатель y_1 , вычислим апостериорные вероятности гипотез для одного свидетельства по формуле (3):

$$P(\alpha_i / y_i) = \frac{P(y_i / \alpha_i)P(\alpha_i)}{\sum_{i=1}^{n} P(y_i / \alpha_i)P(\alpha_i)} \qquad (3)$$

Подставив требуемые значения в (3), получим $P(\alpha_1/y_1) = 0{,}64$; $P(\alpha_2/y_1) = 0{,}31$; $P(\alpha_3/y_1) = 0{,}05$.

Таким образом, после того, как была реализована угроза y_1, доверие к гипотезам α_1 и α_2 возросло, а к гипотезе α_3 – снизилось. Очевидно, что если в результате опыта выяснилось, что СЗИ

не обеспечила конфиденциальность информации при воздействии угрозы, то необходимо рассматривать противоположные события $P(\overline{y_1}/\alpha_i) = 1 - P(y_1/\alpha_i)$. Тогда получим $P(\alpha_1/\overline{y_1}) = 0{,}54$, $P(\alpha_2/\overline{y_1}) = 0{,}16$, $P(\alpha_3/\overline{y_1}) = 0{,}31$.

Таким образом, доверие к гипотезе о низкой защищенности исследуемого ресурса существенно возрастает, а доверие к гипотезе о высокой степени надежности резко уменьшается.

В процессе сбора фактов вероятности гипотез будут повышаться, если факты поддерживают их, или уменьшаться, если факты опровергают их. Если одновременно получены два показателя y_1 и y_2, т.е. установлено, что обеспечены конфиденциальность и целостность, то при условии их независимости можно воспользоваться формулой

$$P(\alpha_i / y_1 y_2) = \frac{P(y_1/\alpha_i)P(y_2/\alpha_i)P(\alpha_i)}{\sum_{i=1}^{3} P(y_1/\alpha_i)P(y_2/\alpha_i)P(\alpha_i)}. \quad (4)$$

Рассчитаем вероятности гипотез $P(\alpha_1/y_1,y_2)$, $P(\alpha_2/y_1,y_2)$ и $P(\alpha_3/y_1,y_2)$ по формуле (4): $P(\alpha_1/y_1,y_2) = 0{,}65$, $P(\alpha_2/y_1,y_2) = 0{,}35$, $P(\alpha_3/y_1,y_2) = 0{,}003$.

По сравнению с результатами, полученными по одному показателю y_1, доверие к первой и второй гипотезам возросло, а к третьей – снизилось. Исходя из этого, с вероятностью 0,35 исследуемый ресурс можно отнести к группе ресурсов с высокой степенью защищенности по отношению к воздействию угрозы типа *Y*. При получении показателя y_3 расчеты проводятся аналогично.

Осуществив подобные расчеты для всех угроз безопасности в соответствии с моделью угроз и зная требования по обеспечению моделей безопасности, можно принимать обоснованные решения по функционированию ресурсов той или иной степени защищенности, а также, при необходимости, конфигурировать СЗИ для ресурсов различных групп.

Этап 5. Оценка последствий нарушения ИБ для каждого типа информационного актива е-кластера. Для оценки степени возможного ущерба от реализации угрозы ИБ определяются возможный результат реализации угрозы ИБ в информационной системе, вид ущерба, к которому может привести реализация угрозы ИБ, степень последствий от реализации угрозы ИБ для каждого вида ущерба.

В качестве результата реализации угрозы ИБ рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе.

Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации: экономический (потеря финансовых средств, недополучение ожидаемой прибыли, необходимость дополнительных затрат на выплаты штрафов или компенсаций и т.п.); социальный (появление негативных публикаций в СМИ, увольнения и т.п.); репутационный (ущерб деловой репутации, снижение престижа, дискредитация персонала и т.п.); технологический (невозможность решения задач, принятие неправильных решений и т.п.).

Степень возможного ущерба обычно определяется экспертным методом и оценивается как «высокая» (невозможность реализации требуемых функций), «средняя» (невозможность реализации минимум одной функции) или «низкая» (незначительные отрицательные последствия).

Заключение

Рассмотрен алгоритм реализации оценки рисков информационной безопасности е-кластеров, основанный на следующих этапах: составление перечня информационных активов е-кластера и соответствующих им типов среды; разработка актуальных источников угроз информационной безопасности е-кластера с оценкой рисков их реализации; осуществление процедур минимизации рисков информационной безопасности е-кластера; осуществление контроля за формированием и динамическим изменением угроз информационной безопасности е-кластера; оценка последствий нарушения информационной безопасности для каждого типа информационного актива е-кластера. Реализация предлагаемого алгоритма позволяет оценить

и управлять рисками информационной безопасности е-кластера с учетом их динамического изменения.

Данный алгоритм лежит в основе методики оценки рисков информационной безопасности е-кластера, базирующейся на байесовском подходе. Данная методика может использоваться для определения вероятности отнесения исследуемых типов ресурсов к группе ресурсов с высокой или низкой степенью защищенности по отношению к воздействию угрозы типа *Y*, что позволяет принимать обоснованные решения по функционированию ресурсов той или иной степени защищенности, а также, при необходимости, конфигурировать систему защиты информации для ресурсов различных групп.

Список литературы

1. Концепция электронной экономики // Электронная экономика: теория, модели, технологии: Т.Н. Беляцкая [и др.]; под общ. ред. Т.Н. Беляцкой, Л.П. Князевой. Минск : БГУИР, 2016. 252 с.
2. СТБ 34.101.41-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения.
3. СТБ 34.101.61-2013. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности.
4. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа. 2012. № 1 (25). Ч. 2. С. 83–86.
5. Зикратов И.А. Одегов С.В., Смирных А.В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 1 (83). С. 141–144.
6. Зикратов И.А., Одегов С.В. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 4 (80). С. 121–126.

References

1. Koncepcija jelektronnoj jekonomiki // Jelektronnaja jekonomika: teorija, modeli, tehnologii: T.N. Beljackaja [i dr.]; pod obshh. red. T.N. Beljackoj, L.P. Knjazevoj. Minsk : BGUIR, 2016. 252 s. (in Russ.)
2. STB 34.101.41-2013. Informacionnye tehnologii i bezopasnost'. Obespechenie informacionnoj bezopasnosti bankov Respubliki Belarus'. Obshhie polozhenija. (in Russ.)
3. STB 34.101.61-2013. Informacionnye tehnologii i bezopasnost'. Obespechenie informacionnoj bezopasnosti bankov Respubliki Belarus'. Metodika ocenki riskov narushenija informacionnoj bezopasnosti. (in Russ.)
4. Pletnev P.V. Metodika ocenki riskov informacionnoj bezopasnosti na predprijatijah malogo i srednego biznesa / P.V. Pletnev, V.M. Belov // Doklady TUSURa. 2012. № 1 (25). Ch. 2. S. 83–86. (in Russ.)
5. Zikratov I.A. Ocenka riskov informacionnoj bezopasnosti v oblachnyh servisah na osnove linejnogo programmirovanija / I.A. Zikratov, S.V. Odegov, A.V. Smirnyh // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2013. № 1 (83). S. 141–144. (in Russ.)
6. Zikratov I.A. Ocenka informacionnoj bezopasnosti v oblachnyh vychislenijah na osnove bajesovskogo podhoda // I.A. Zikratov, S.V. Odegov // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2012. № 4 (80). S. 121–126. (in Russ.)

Сведения об авторах

Лыньков Л.М., д.т.н., профессор, профессор кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Беляцкая Т.Н., к.э.н., доцент, зав. кафедрой менеджмента Белорусского государственного университета информатики и радиоэлектроники.

Князькова В.С., магистр технических наук, преподаватель кафедры менеджмента Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Lynkov L.M., D. Sci., professor, professor of the information security department of Belarusian state university of informatics and radioelectronics.

Beliatskaya T.N., PhD, associate professor, chief of management department of Belarusian state university of informatics and radioelectronics.

Knyazkova V.S., M. Sci., assistant of management department of Belarusian state university of informatics and radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, д. 6,
Белорусский государственный
университет информатики и радиоэлектроники
тел. +375-17-293-86-46;
e-mail: knyazkova@bsuir.by;
Князькова Вероника Святославовна

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian State University
of Informatics and Radioelectronics
tel. +375-17-293-86-46;
e-mail: knyazkova@bsuir.by;
Knyazkova Veronika Sviatoslavovna