4. *Ali A. Hamzah, Sherif Khattab, Hanaa Bayomi*. A Linguistic Steganography Framework Using Arabic Calligraphy: Journal of King Saud University-Computer and Information Sciences. 2019. Vol. 8. P. 4–17.
5. *Bonnie Dorr, Matt Snover, Nitin Madnani*. Machine Translation Evaluation. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.348.5771 (date of the application: 06.05.2020).
6. *Ching-Yun Chang, Stephen Clark*.The Secret's in the Word Order: Text-to-Text Generation for Linguistic Steganography // Proc. of COLING 2012. [S. l.], 2012. P. 511–528.
7. *Ching-Yun Chang, Stephen Clark*. Practical Linguistic Steganography using Contextual Synonym Substitution and a Novel Vertex Coding Method // Computational Linguistics. 2014. Vol. 40. P. 403–448.
8. *Philipp Koehn*. Statistical Machine Translation. [S. l.], 2010. 433 p.
9. *Topkara M., Topkara U., Atallah M.J.* Words are Not Enough: Sentence Level Natural Language Watermarking // MCPS '06: Proc. of the 4th ACM International Workshop on Contents Protection and Security. [S. l.], 2006. P. 37–46.
10. *Zachary M. Ziegler, Yuntian Deng, Alexander M. Rush*. Neural Linguistic Steganography // Proc. of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP). [S. l.], 2019.

DOI: 10.25586/RNU.V9187.20.02.P.080 УДК 004.94

К.А. Эсаулов, Е.К. Яхваров, А.А. Нечай, А.С. Березин

# МЕТОДИКА ИНТЕГРАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ КИБЕРРИСКАМИ В ПРЕДПРИНИМАТЕЛЬСКИХ СТРУКТУРАХ

Рассмотрено влияние информационных рисков на деятельность предпринимательских структур. Рассмотрен алгоритм интеграции управления киберрисками в общую систему управления предпринимательской структурой. Алгоритм предполагает анализ возможных альтернатив интеграции управления киберрисками с учетом возможных ошибок при принятии решений и соответствующего ущерба. Внедрение предложенного алгоритма возможно при стратегическом планировании, бюджетировании, осуществлении контроля, мониторинга и оценки эффективности деятельности предпринимательской структуры. Использование предложенного алгоритма позволит повысить эффективность противодействия киберпреступности.
*Ключевые слова:* предпринимательская структура, риск-менеджмент, киберриск, кибербезопасность, четвертая промышленная революция.

K.A. Esaulov, E.K. Yakhvarov, A.A. Nechai, A.S. Berezin

# METHODOLOGY FOR INTEGRATING THE CYBER RISK MANAGEMENT SYSTEM IN BUSINESS STRUCTURES

The article considers the impact of information risks on the activities of business structures. An algorithm for integrating cyber risk management into the overall business structure management system is considered. The algorithm analyzes possible alternatives to integrating cyber risk management, taking

into account possible errors in decision-making and the corresponding damage. Implementation of the proposed algorithm is possible in strategic planning, budgeting, control, monitoring and evaluation of the effectiveness of the business structure. Using the proposed algorithm will increase the effectiveness of countering cybercrime.

*Keywords:* business structure, risk management, cyber risk, cybersecurity, the fourth industrial revolution.

## *Введение*

Основные масштабные изменения, происходящие в мировой экономике, связанны с высоким темпом развития научно-технологического прогресса, спровоцированные новой четвертой промышленной революцией. Технологии, обеспечивающие четвертую промышленную революцию [1; 5], влияют на форму и качество продуктов и услуг, формируют поведение потребителей, создают новые модели роста коммерческих компаний. Искусственный интеллект – одна из технологий, относящаяся к цифровой промышленной революции [8; 9], – по оценке Глобального института McKinsey, позволит к 2030 г. создать экономический эффект для мировой экономики в размере 13 трлн долларов в год [2]. По оценке того же института, в течение 20 лет 50% операций в мире будут автоматизированы. Глобальные технологические преобразования цифровой революции не только приведут к автоматизации бизнес-процессов, повышая производительность труда [4] (ежегодный темп роста производительности труда составит 2,3% в течение 2025–2030 гг. по данным консалтинговой аудиторской кампании Deloitte) [3], но и будут сопровождаться новыми рисками, связанными с этими изменениями [6] («кибератаки», «кража данных»). По данным отчета Всемирного экономического форума «Глобальные риски» WEF (World Economic Forum) за 2019 г., экономический ущерб от киберпреступности к 2020 г. достигнет 3 трлн долларов. В 2017 г. убытки российских компаний из-за кибератак составили 116 млрд руб. Наиболее распространенные последствия киберпреступлений представлены на рисунке 1. Среди распространенных последствий киберпреступлений лидируют: нарушение бизнес-процессов операций (68%), ущербы для репутации (58%), финансовые убытки (45%).

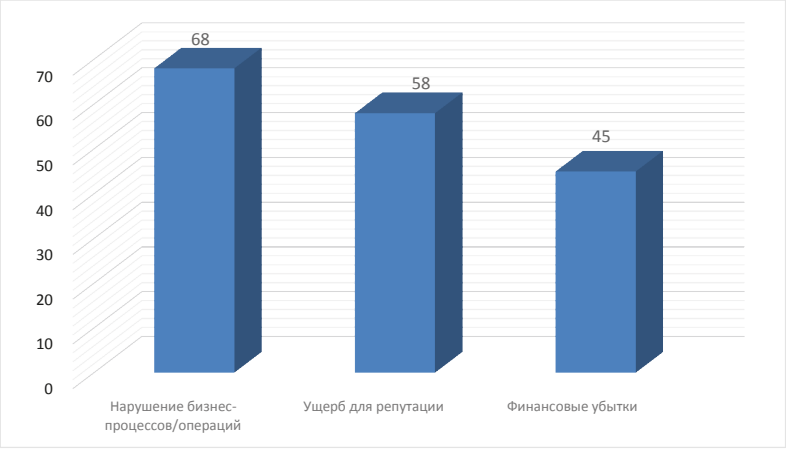


**Рис. 1.** Наиболее распространенные последствия киберпреступлений, %

Предпринимательским структурам следует активно отслеживать угрозы и обеспечивать устойчивость бизнеса. Для этого необходимо интегрировать систему управления рисками в систему управления коммерческих организаций.

Риски, с которыми сталкивается предприятие в цифровой области, должны быть проанализированы и классифицированы в рамках системы киберрисков. Как только киберриски будут более четко пониматься как бизнес-риски, возникающие в цифровой области, организация будет правильно ориентирована на то, чтобы приступить к реализации подхода, основанного на оценке риска.

Интеграция управления киберрисками состоит из 4 основных мероприятий (рис. 2).

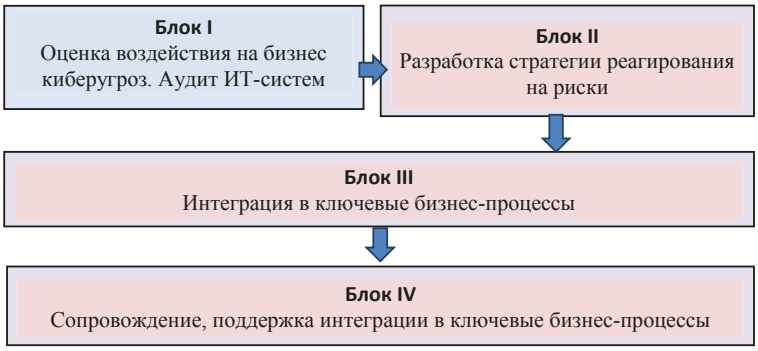


**Рис. 2.** Интеграция управления киберрисками

Блок I этого методического обеспечения содержит методику оценки воздействия на бизнес киберугроз; включает аудит ИТ-систем. Первый блок начинается с анализа ключевых бизнес-процессов, выбора мероприятий по воздействию на них с целью выявления рисков следующей группы – персонала, помещений, поставщиков, данных.

Блок II содержит разработку стратегии реагирования на риски. В зависимости от выявленной уязвимости, которая создает угрозу, необходимо сопоставить меры и средства, направленные на ее устранение.

Блок III содержит процесс разработки плана по реализации стратегии. Применение мер и средств, направленных на парирование угрозы, связано с дополнительными затратами. Выбор одного из альтернативных решений должен быть обоснован с учетом затрат и возможных потерь в случае реализации угрозы.

Блок IV этого методического обеспечения содержит процесс сопровождения и поддержки интеграции в ключевые бизнес-процессы. Внедрение выбранного решения по противодействию киберугрозам не окончательный шаг, и необходимо контролировать его эффективность и оперативно реагировать на происходящие изменения. Система должна поддерживаться в актуальном состоянии, чтобы быть способной противостоять вновь появляющимся угрозам.

Объединив данные четырех блоков, получим комплексное методическое обеспечение, необходимое для противодействия киберугрозам. Наиболее важным является блок III, так как он связан с обоснованием выбора решения. Предлагается следующая постановка задачи.

Пусть дан набор альтернативных решений до интеграции управления рисками в систему управления организации:

$$Y = \{y_1, y_2, y_3, \ldots, y_N\},$$

где $Y$ – набор альтернативных решений, состоящий из $y_1, y_2, y_3, \ldots, y_N$; $N$ – количество альтернативных решений.

Последствия ошибки в принятии решения могут быть оценены величиной $(C)$, выраженной в стоимостном отношении в виде суммы стоимостей прямого $(C_{\text{пр. ущ}})$ и косвенного ущерба $(C_{\text{косв. ущ}})$:

$$C = C_{\text{пр. ущ}} + C_{\text{косв. ущ}}.$$

Вероятность ошибки характеризуется величиной, состоящей из вероятностей неверных действий, приводящих к общей ошибке:

$$Q_0(q_{10}, q_{20}, \ldots, q_{N0}) = 1 - P_0,$$

где $Q_0$ – вероятность ошибки; $q_{10}, q_{20}, \ldots, q_{N0}$ – набор неверных действий, приводящих к $Q_0$; $P_0$ – вероятность безошибочной работы организации.

$$C_{\text{ущ}} = Q_0(C_{\text{пр. ущ}} + C_{\text{косв. ущ}}).$$

Для каждой бизнес-цели и реализации соответствующего решения из набора $\{y_1, y_2, y_3, \ldots, y_N\}$ существует риск, т.е. $\{r_1, r_2, r_3, \ldots, r_N\}$.

Составим для такого набора профиль риска (рис. 3).

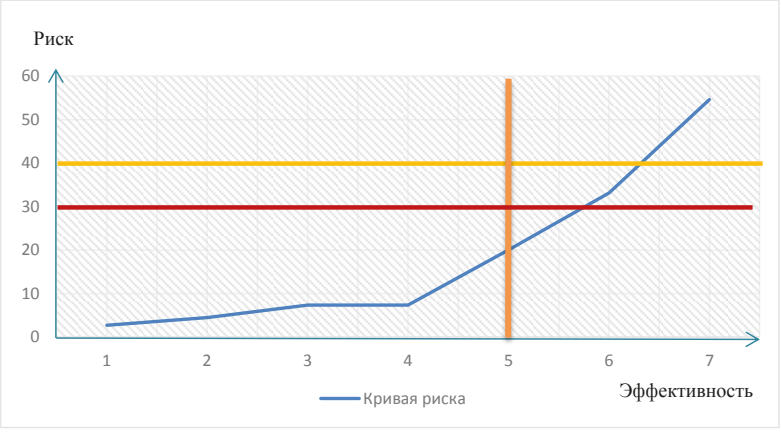


**Рис. 3.** Профиль риска (условное изображение)

Интеграция алгоритма по управлению риском значительно снизит вероятность ошибки в принятии решения. Это может быть реализовано посредством следующих мероприятий:

- оценка воздействия на бизнес киберугроз, аудит ИТ-систем – $X_1$;
- разработка плана по реализации стратегии – $X_2$;
- интеграция в ключевые бизнес-процессы – $X_3$;
- сопровождение поддержка и процедуры – $X_4$.

Управленческое решение будет состоять в векторе *X*:

$$X = \left(X_1, X_2, X_3, X_4\right),$$

где $X_1, X_2, X_3, X_4$ – определенные величины, для которых существует набор значений.

Методом экспертных оценок для каждой из величин $X_1, X_2, X_3, X_4$ выбирается набор значений, т.е. для $X_1$:

$$X_1 \in \left\{a_{11}, a_{12}, \ldots, a_{1k_1}\right\},$$

где *a* – один из вариантов внедрения управления рисками в стратегическое планирование; $k_1$ – количество вариантов *a* для стратегического планирования.

Аналогично для $X_2, X_3, X_4$ :

$$X_2 \in \left\{a_{21}, a_{22}, \ldots, a_{2k_2}\right\};$$

$$X_3 \in \left\{a_{31}, a_{32}, \ldots, a_{3k_3}\right\};$$

$$X_4 \in \left\{a_{41}, a_{42}, \ldots, a_{4k_4}\right\}.$$

Таким образом, всего управленческих решений

$$k_{\text{общ}} = k_1 k_2 k_3 k_4.$$

Для каждого из этих вариантов производим сужение набора $Y$ (с помощью экспертной оценки исходя из состояния рынка отрасли, в которой компания ведет деятельность, размера компании, анализа финансово-хозяйственной деятельности):

$$x = \left(a_{1i}, a_{2j}, a_{3l}, a_{4z}\right),\ i \in \left\{1, \ldots k_1\right\},\ j \in \left\{1, \ldots k_2\right\},\ l \in \left\{1, \ldots k_3\right\},\ z\left\{1, \ldots k_4\right\}.$$

Проведя мероприятия $X$, получим $Y_{ijlz}$, т.е. $Y \to Y_{ijlz}$, где $Y_{ijlz}$ – новый набор альтернативных решений при этом наборе интеграционных мероприятий по управлению рисками $x = \left(a_{1i}, a_{2j}, a_{3l}, a_{4z}\right)$.

Каждая из альтернатив характеризуется затратами $S_{i,y,l,z}$ :

$$S_{i,y,l,z} i \in \left\{1, \ldots, k_1\right\},\ j \in \left\{1, \ldots k_2\right\},\ l \in \left\{1, \ldots k_3\right\},\ z \in \left\{1, \ldots k_4\right\};$$

$$\left[x_i, x_j, x_l, x_z\right] \in \left\{a_{i1}, a_{i2}, \ldots, a_{ik_i};\ a_{y1}, a_{y2}, \ldots, a_{yk_i};\ a_{z1}, a_{z2}, \ldots, a_{zk_i}\right\} \forall i, j, l, z = 1...n;$$

$$S(X) = \sum_{i=1}^{n} S_{ijlz}\left(x_{ijlz}\right).$$

Повышение вероятности $p(t)$ безотказного функционирования (верного решения) осуществляется методом экспертной оценки путем выбора набора альтернатив $x_i$ из $\left\{a_{i1}, a_{i2}, \ldots a_{ik_i}\right\}$, $x_y$ из $\left\{a_{y1}, a_{y2}, \ldots a_{yk_i}\right\}$, $x_z$ из $\left\{a_{z1}, a_{z2}, \ldots a_{zk_i}\right\}$. Каждая из $k_{iyz}$ альтернатив характеризуется затратами $S_{iyz}$ на ее осуществление. Требуется на множестве $\left[x_i, x_y, x_z\right]$ допустимых значений найти такое значение X, при котором ущерб минимален, а полученные затраты были меньше запланированных:

$$X = \arg\min\left(C_{\text{ущ}}(X) \middle| S(X) = \sum_{i,y,z=1}^{N} s(x) \le S_{\text{зад}}\right.$$

Актуальная информация о киберрисках будет регулярно предоставляться руководству компании для принятия стратегически важных решений. Развитие процессов риск-ме-

неджмента в кибербезопасности позволит предпринимательским структурам быть высокотехнологичными компаниями с быстрыми, удобными и безопасными сервисами, несмотря на растущий интерес со стороны киберпреступников [7]. Создание единой системы менеджмента киберрисков и их оценки будет способствовать в дальнейшем объединению усилий в борьбе с киберпреступностью.

## Литература

1. *Борисов А.А., Краснов С.А., Нечай А.А.* Технология блокчейн и проблемы ее применения в различных информационных системах // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. Вып. 2. С. 63–63.
2. Методологические основы оценки военно-экономической эффективности управленческой деятельности: учебное пособие / А.Л. Михайлов и др. СПб.: ВАТТ, 2004. 230 с.
3. *Нечай А.А.* Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. 2019. № 4. С. 43–44.
4. *Нечай А.А., Борисов А.А., Борисова Ю.И.* Точечный анализ данных дистанционного зондирования Земли средствами языка программирования Python // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. Вып. 1. С. 49–55.
5. *Нечай А.А., Копьев А.И.* Метод управляемого распределения ресурсов между ядрами процессора // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. Вып. 2. С. 101–106.
6. *Пименова А.Л, Эсаулов К.А., Яхваров Е.К.* Совершенствование системы контроллинга в предпринимательских структурах в условиях цифровизации // Петербургский экономический журнал. Экономика и управление хозяйствующими субъектами. 2019. № 3. С. 14–23.
7. Разработка классификации и системы показателей оценивания рискоустойчивостей предприятий при достижении тактико-технических требований в ходе выполнения гособоронзаказа / Е.К. Яхваров и др. // Проблемы в экономике и юридической практике. 2015. № 5. С. 215–218.
8. *Свинарчук А.А., Нечай А.А.* Использование квантовых вычислений при выборе управленческого решения // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2018. Вып. 2. С. 31–36.
9. *Шаймарданов А.М., Нечай А.А., Лепехин С.В.* Математическая модель систем автоматического управления с широтно-импульсной модуляцией // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. Вып. 2. С. 27–39.

## Literatura

1. *Borisov A.A., Krasnov S.A., Nechaj A.A.* Tekhnologiya blokchejn i problemy ee primeneniya v razlichnykh informatsionnyh sistemakh // Vestnik Rossijskogo novogo universiteta. Seriya “Slozhnye sistemy: modeli, analiz i upravlenie”. 2018. Vyp. 2. S. 63–63.
2. Metodologicheskie osnovy otsenki voenno-ekonomicheskoj effektivnosti upravlencheskoj deyatel’nosti: uchebnoe posobie / A.L. Mihajlov i dr. SPb.: VATT, 2004. 230 s.
3. *Nechaj A.A.* Formirovanie bezopasnoj informatsionnoj sredy // Aktual’nye problemy sovremennosti: nauka i obshchestvo. 2019. № 4. S. 43–44.

4. *Nechaj A.A., Borisov A.A., Borisova Yu.I.* Tochechnyj analiz dannykh distantsionnogo zondirovaniya Zemli sredstvami yazyka programmirovaniya Python // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 1. S. 49–55.
5. *Nechaj A.A., Kop'ev A.I.* Metod upravlyaemogo raspredeleniya resursov mezhdu yadrami protsessora // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2018. Vyp. 2. S. 101–106.
6. *Pimenova A.L, Esaulov K.A., Yahvarov E.K.* Sovershenstvovanie sistemy kontrollinga v predprinimatel'skikh strukturakh v usloviyakh tsifrovizatsii // Peterburgskij ekonomicheskij zhurnal. Ekonomika i upravlenie hozyajstvuyushchimi sub"ektami. 2019. № 3. S. 14–23.
7. Razrabotka klassifikatsii i sistemy pokazatelej otsenivaniya riskoustojchivostej predpriyatij pri dostizhenii taktiko-tekhnicheskikh trebovanij v hode vypolneniya gosoboronzakaza / E.K. Yakhvarov i dr. // Problemy v ekonomike i yuridicheskoj praktike. 2015. № 5. S. 215–218.
8. *Svinarchuk A.A., Nechaj A.A.* Ispol'zovanie kvantovykh vychislenij pri vybore upravlencheskogo resheniya // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2018. Vyp. 2. S. 31–36.
9. *Shajmardanov A.M., Nechaj A.A., Lepekhin S.V.* Matematicheskaya model' sistem avtomaticheskogo upravleniya s shirotno-impul'snoj modulyatsiej // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2019. Vyp. 2. S. 27–39.

DOI: 10.25586/RNU.V9187.20.02.P.086 УДК 681.3

Д.Е. Орлова

# АЛГОРИТМЫ КООРДИНАЦИОННОГО УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Предложены алгоритмы управления комплексной безопасностью объектов критического применения, отличающиеся от аналогов тем, что при их построении классические модели оптимизации дополняются координационными моделями, позволяющими учесть многокритериальность, иерархичность и взаимосвязанность компонентов управляемых объектов.
*Ключевые слова:* безопасность, управление, координация, алгоритм, выходной интерфейс, сходимость.

D.E. Orlova

# ALGORITHMS FOR COORDINATING MANAGEMENT OF COMPLEX SECURITY OF CRITICAL APPLICATION OBJECTS

Algorithms for managing the complex security of critical objects are proposed. they differ from their analogues in that the classical optimization models are supplemented with coordination models that allow taking into account the multi-criteria, hierarchy and interconnectedness of the components of managed objects.
*Keywords*: security, management, coordination, algorithm, output interface, convergence.