Анализ эффективности системы управления информационной безопасностью государственного учреждения

Analyzing the Efficiency of a Governmental Information Security Management System

УДК 35:004

Серова Анастасия Геннадьевна
аспирант Санкт-Петербургского университета технологий управления и экономики
190103, Санкт-Петербург, Лермонтовский пр., д. 44, лит. А

Anastasiya G. Serova
St. Petersburg University of Management Technologies and Economics
Lermontovskiy Ave 44/A, St. Petersburg, Russian Federation, 190103

Цель. Определить комплекс мероприятий, направленных на эффективное функционирование анализируемой системы управления информационной безопасностью государственного учреждения (СУИБ ГУ). На основании оценок данной системы управления предложить управленческие решения.
Задачи. Разработать комплекс мероприятий, полученных в ходе оценки мероприятий по регулированию рисков ИБ, направленных на совершенствование управленческих решений и СУИБ.
Методология. В настоящей работе с помощью общих методов научного познания, метода экспертных оценок и с применением статистических методов обработки данных разработаны предложения по совершенствованию функционирования системы управления управленческими решениями.
Результаты. В данной статье представлены итоги опытно-экспериментальной процедуры аудита СУИБ. Для получения оценок текущего состояния СУИБ ГУ был использован системный подход.
Выводы. В ходе проведенного анализа был идентифицирован основной риск ИБ — социальная и экономическая безопасность сотрудника, отвечающего за ИБ в учреждении. Управленческое решение должно быть направлено на совершенствование СУИБ ГУ с помощью рекомендаций по совершенствованию ресурсов для обеспечения функционирования данной системы управления.
Ключевые слова: система управления информационной безопасностью (СУИБ), информационная безопасность (ИБ), государственное учреждение (ГУ), сотрудник, ответственный за ИБ (СИБ)

Aim. This study is dedicated to the determination of a set of measures aimed at ensuring the efficient functioning of the information security management system (ISMS) of a government agency (GA) and proposing managerial solutions on the basis of the assessment of the system.
Tasks. This study develops a set of measures obtained during the assessment of information security (IS) risk control measures aimed at improving managerial decisions and ISMS.
Methods. This study uses general scientific-cognition, expert assessment, and statistical data-processing methods to develop proposals for improving managerial decision management.
Results. This study presents the results of an experimental ISMS audit procedure using a systems approach for obtaining assessments of the current state of the ISMS of a GA that includes the legislative, administrative, technical, organizational, and social components.
Conclusion. The social and economic security of the IS administrator represents the main IS risks. Managerial decisions should be aimed at improving the ISMS of a GA through guidelines for the improvement of resources with the purpose of ensuring the functioning of the management system.
Keywords: information security management system (ISMS), information security (IS), government agency (GA), IS administrator (ISA)

Сегодня аудит в системах управления информационной безопасностью (СУИБ), по мнению автора, считается основной областью для исследований и постановок новых задач в этой области. В том числе возрастает интерес к эффективным и современным методам анализа и управления в СУИБ государственных учреждений (ГУ). Возникает необходимость в увеличении ресурсов и разработке новых методов решения возникающих проблем [1]. Труд-

ности возникают из-за неизбежно растущих рисков и угроз информационной безопасности, что является результатом совершенствования информационных процессов [2].

Существуют серии стандартов, в которых регламентируются требования к анализу и управлению рисками информационной безопасности (ИБ). Это международные и национальные стандарты оценок рисков и управления: ISO 15408, ISO 17799 (BS 7799), ISO 27001(X), BSI и стандарты, отражающие вопросы ИБ: COBTI, SAC, COSO, SAS 55/78, Германский стандарт BSI и BSI — Standarts 100-3 [3] и т. д.

Стандарты, прежде всего, затрагивают законодательную, административную и техническую компоненты [4, с. 29] СУИБ. Существование данных стандартов не означает, что в области управления ИБ разрешены все задачи и проблемы. Главной составляющей СУИБ является организационно-экономическая компонента. Она служит для гарантии работоспособности СУИБ, внедрения и управления необходимыми и достаточными ресурсами (среди которых — социальные, психологические). В разработанной методике все принятые управленческие решения для регулирования рисков ИБ основываются на математических методах оценки рисков ИБ и системном анализе СУИБ, которая представляет собой совокупность компонент: законодательной, организационной, технической и социально-психологической.

Такие западные ученые, как Т. Питерс, У. Оучи, Э. Этос, С. Джонсон, Т. Дил, Г. Пинию, З. Кеннеди, Р. Уотерман, Р. Паскаль, К. Баншир, являются известными специалистами в области менеджмента. Изучая их работы, связанные с ИБ в организациях, мы выяснили, что сохранность и конфиденциальность информации зависят не только от подбора, воспитания и расстановки кадров, но и от безошибочно принятого управленческого решения. «Люди — самый ценный ресурс в организации, это основной ресурс производительности». Данная позиция олицетворяет интерес в области менеджмента к человеческому фактору. Сегодня человек — основная производительная сила в социуме. Почти все мнения ученых и теории, посвященные менеджменту, сводятся к тому, что в настоящее время возрастает роль человеческого фактора [5]. Зарождается интерес в использовании физических, эмоциональных и психологических возможностей сотрудников, их творческого, исполнительного и организаторского потенциалов.

СУИБ государственных учреждений и все вопросы и проблемы, связанные с ее преобразованием и эффективностью, полностью не исследованы. Такие исследователи, как Д. С. Черешкин, Г. Л. Смолян, Д. П. Зегжда, А. А. Кононов, В. И. Аверченков, А. А. Стрельцов, А. А. Варфоломеев, А. Г. Ростовцев, Т. А. Казакевич, С. П. Расторгуев и др., внесли свой вклад в процесс организации, развития и функционирования СУИБ. Мы базировались на их выводах. Наше исследование осуществлено с применением принципов системного анализа, SWOT-анализа, метода структуризации, методов экспертного опроса и статистических методов обработки итогов экспертного опроса.

При решении проблем и задач в области аудита и управления рисками ИБ также используются средства и методы системного анализа СУИБ [6; 7]. В своем исследовании автор представляет теоретические основы аудита СУИБ и разработанную методику аудита и управления СУИБ ГУ. Для этого была осуществлена опытно-экспериментальная процедура аудита СУИБ ГУ.

Первый организационный этап процедуры аудита заключается в выборе организации для исследования в соответствии с поставленными задачами. На данном этапе рассматривается контингент испытуемых, также цели экспертизы и сроки завершенной процедуры аудита. Целью экспертизы является аудит СУИБ и исследование рисков ИБ. По завершении данного анализа рисков ИБ представится возможность получить рекомендации по совершенствованию СУИБ при помощи регулирования рисков и принятия правильного управленческого решения.

Второй этап служит для того, чтобы сформировать группу экспертов-аналитиков и ее состав. Все специалисты, которые приглашались на анкетирование, заслуживают доверия и являются экспертами в сфере ИБ. Группа, в нашем случае, состоит из 14 экспертов-аналитиков, которые являются специалистами подразделений ИТ и ИБ. С целью обоснования численности экспертов в группе были проведены работы по непосредственному подбору ее состава. Высокая квалификация специалиста считается очень значимым условием, она оказывает влияние на достоверность. Мы рассчитали Q_i — интегральную оценку коэффициента компетентности:

$$Q_i = 0{,}5 \cdot \left(\frac{\sum_{j=1}^{m} K_j}{\sum_{j=1}^{m} K_j^{\max}} + \frac{q}{q^{\max}} \right), \qquad (1)$$

где K_j — документально подтвержденная оценка специалиста по его j-й характеристике; $K_j^{\max}$ — максимально возможная оценка по j-й характеристике; q — самооценка специалиста по проблеме в целом; $q^{\max}$ — максимально возможная оценка по проблеме в целом.

Как уже было указано, с использованием вышеуказанной формулы нами было отобрано 14 экспертов-аналитиков из 20 кандидатов.

Третий оценочный этап представляет из себя сам процесс аудита. Он направлен на раскрытие слабых и сильных качеств СУИБ по ее компонентам (законодательный, административный, технический и организационный, включающий в себя социально-психологический компонент).

1. По результатам исследования законодательная компонента в анализируемом учреждении соответствует требованиям. Для регулирования требований, связанных с обработкой информации, используются данные с ограниченным доступом. Учитываются постановления правительства, законы, указы президента, стандарты и нормативные акты. Находят применение меры ответственности за несоблюдение установленных требований.
2. Анализируя административную компоненту, мы установили, что исследуемое учреждение содержит всю документацию, содержащую в себе необходимые политики ИБ, требования стандартов на соответствие правил ИБ деловой активности учреждения.
3. При исследовании технической компоненты анализировались мероприятия, относящиеся к защите информации в учреждении. Проведены работы по исследованию аппаратных и программных средств ИБ.
4. Исследование организационной компоненты предполагало анализ мероприятий, связанных с внедрением, управлением необходимыми и достаточными ресурсами для обеспечения функционирования СУИБ.

Для исследования использовался метод SWOT-анализа [8], на его основе были предложены мероприятия, направленные на эффективное управление ИБ учреждения. Далее мы применили тактику разделения мероприятий, используя классификационную матрицу мероприятий SWOT-анализа. Данное разделение представляет собой выделение групп мероприятий: внешних и внутренних, контролируемых и неконтролируемых. Далее предлагается сформировать дерево проблем в СУИБ. Это даст возможность получить список факторов, ведущих к причинам рисков ИБ.

Выявление целей — это не только шаг к формированию дерева целей в СУИБ [9]. Выявляя факторы, ведущие к рискам ИБ, мы переходим к следующему шагу — целям в СУИБ. Посредством формирования древа целей СУИБ образуется перечень мероприятий для снижения рисков ИБ. Мероприятия следует осуществить для достижения выявленных целей, используя получившийся перечень работ и действий. Полнота выполнения мероприятия на совершенствование СУИБ — главное условие для оценки СУИБ.

Далее была проведена процедура анкетирования экспертной группы. В анкете для экспертного опроса были зафиксированы все предложенные мероприятия с целью получения оценки важности отобранных мероприятий по усовершенствованию СУИБ и принятия правильного управленческого решения. Так как тематика опроса требует конфиденциальности, опрос проводился анонимно. Если в ходе опроса имелись предложения со стороны экспертов-аналитиков, после первого этапа опроса каждый следующий этап проходил с учетом новых предложений от предыдущего опроса.

Суть действий экспертов состояла в назначении нечисловым характеристикам (мероприятиям) количественных или качественных оценок. Так как количество экспертов в опросе — 14, значение оценок варьировалось от 1 до 14. Далее, с применением статистических методов обработки, анализировались данные, полученные в ходе анкетирования.

Нами определился относительный вес W_n (2) каждого мероприятия по всем экспертам [10]. Для этого рассчитывались суммы стандартизированных рангов по всем экспертам $\sum SR_n$.

$$W_n = \frac{SR_n}{\sum_{j=1}^{m} SR_n}, \qquad (2)$$

где $\sum_{j=1}^{m} W_n = 1$.

Также мы вычислили коэффициент конкордации Кендала:

$$V = \frac{12S}{m^2 \cdot (n^3 - n)}. \qquad (3)$$

В результате использованной процедуры нестрогого ранжирования, максимальное значение дисперсии оказывается меньше, чем у связанных рангов, поэтому формула для определения коэффициента конкордации корректируется. В данной ситуации коэффициент конкордации вычислялся по формуле:

$$V = \frac{12}{\frac{1}{12} \cdot n^2 \cdot (m^3 - m) - n \cdot \sum_{k=1}^{h} T_i}, \qquad (4)$$

где m_j — количество экспертов; n_j — число факторов; h_k — число равных рангов в k-й группе связанных рангов в ранжировке, полученной от j-го эксперта; T_j — показатель связанных рангов, число групп равных рангов в j-й ранжировке:

$$T_j = \sum_{k=1}^{H} (h_k^3 - h_k). \qquad (5)$$

Отклонение суммы рангов от среднего значения суммы рангов определялось как:

$$S = \sum\sum_{i=1}^{m} \left(SR_n - \frac{1}{n} \cdot \sum_{i=1}^{n}\sum_{j=1}^{m} SR_n \right)^2; \qquad (6)$$

$\left(\frac{1}{n}\cdot\sum_{i=1}^{n}\sum_{j=1}^{m}SR_n\right)$ — среднее значение суммы рангов (7),

где D_i — разность суммы рангов и среднего значения суммы рангов.

Далее нами рассчитывался критерий Пирсона ($\lambda_p^2 > \lambda_t^2$) для определения уровня значимости коэффициента конкордации Кендала:

- если ранги несвязанные, то:

$$\lambda_p^2 = n\cdot(m-1)\cdot V; \quad (8)$$

- при связанных рангах:

$$\lambda_p^2 = \frac{S}{\frac{1}{12}\cdot m\cdot n\cdot(n-1)-\frac{1}{n-1}\cdot\sum_{i=1}^{n}T_j}. \quad (9)$$

При условии выполнения требования ($\lambda_p^2 > \lambda_t^2$) гипотеза о согласованности мнений принимается, где λ_t^2 — табличное значение коэффициента для степеней свободы $f = m - 1$ и уровня значимости α.

Исследование привело нас к выводу о том, что во главе дерева целей находятся три мероприятия, полученные в ходе оценки мероприятий по регулированию рисков ИБ и направленные на совершенствование управленческих решений и СУИБ.

1. Должность сотрудника, ответственного за ИБ (СИБ), должна быть в иерархии не ниже уровня заместителя начальника того отдела, в чьем подчинении он находится.
2. Требуется изменение психологии СИБ, повышение его самооценки и проявление уважения к нему со стороны всех сотрудников организации на основе проведения бесед руководителя учреждения со всеми сотрудниками, что способствует снижению нарушений трудовой дисциплины, улучшению межличностных отношений, психологического климата коллектива, стиля управления в учреждении.
3. Необходимо пересмотреть систему материального поощрения.

В ходе проведенного анализа был идентифицирован основной риск ИБ — социальная и экономическая безопасность самого СИБ. Управленческое решение по преодолению выявленных проблем должно быть направлено на совершенствование СУИБ ГУ с помощью повышения эффективности использования ресурсов, выделяемых для обеспечения функционирования данной системы управления.

Литература

1. *Цирлов В. Л.* Основы информационной безопасности автоматизированных систем [краткий курс]. Ростов-на-Дону: Феникс, 2008. 253 с.
2. *Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.* Основы управления информационной безопасностью: Учеб. пособие. 2-е изд., испр. М.: Горячая линия-Телеком, 2014. 244 с.
3. *Стрельцов А. А.* Обеспечение информационной безопасности России: Теоретические и методологические основы / Под ред. В. А. Садовничего, В. П. Шерстюка. М.: МЦНМО, 2002. 296 с.
4. *Проблемы* управления информационной безопасностью / Под ред. Д. С. Черешкина. М.: Изд. группа URSS, 2002. 192 с.
5. *Соловьев Д. П.* Энциклопедия управления персоналом: [Электронный ресурс]. Режим доступа: dps.smrtlc.ru.
6. *Варфоломеев А. А.* Управление информационными рисками: Учеб. пособие. М.: РУДН, 2008. 158 с.
7. *Завгородний В. И.* Системное управление информационными рисками. Выбор механизмов защиты // Проблемы управления. 2009. № 1. С. 53–58.
8. *Писарева О. М.* Методы социально-экономического прогнозирования: Учебник. М.: ГУУ-НФПК, 2003. 395 с.
9. *Машунин Ю. К.* Разработка управленческого решения: Учеб. пособие. Владивосток: ТИДОТ ДВГУ, 1999. 111 с.
10. *Егоров А. И.* Основы теории управления. М.: ФИЗМАТЛИТ, 2004. 504 с.

References

1. Tsirlov V. L. *Osnovy informatsionnoy bezopasnosti avtomatizirovannykh sistem. Kratkiy kurs* [Fundamentals of information security of automated systems. A short course]. Rostov-na-Donu: Feniks Publ., 2008. 253 p.
2. Kurilo A. P., Miloslavskaya N. G., Senatorov M. Yu., Tolstoy A. I. *Osnovy upravleniya informatsionnoy bezopasnost'yu* [Fundamentals of information security management]. Moscow: Hotline-Telecom Publ., 2014. 244 p.
3. Strel'tsov A. A. *Obespechenie informatsionnoy bezopasnosti Rossii: teoreticheskie i metodologicheskie osnovy* [Providing information security of Russia: Theoretical and methodological foundations]. Moscow: Moscow Center for Continuous Mathematical Education Publ., 2002. 296 p.
4. Chereshkin D. S., ed. *Problemy upravleniya informatsionnoy bezopasnost'yu* [Information security management issues]. Moscow: Editorial URSS Publ., 2002. 192 p.
5. Solov'ev D. P. *Encyclopedia of personnel management.* Available at: http://dps.smrtlc.ru/. (in Russ.).
6. Varfolomeev A. A. *Upravlenie informatsionnymi riskami* [Information risk management]. Moscow: RUDN Univ. Publ., 2008. 158 p.
7. Zavgorodniy V. I. Sistemnoe upravlenie informatsionnymi riskami. Vybor mekhanizmov zashchity [System management of information risks: Choice of mechanisms for protection against information risks]. *Problemy upravleniya*, 2009, no. 1, pp. 53–58.
8. Pisareva O. M. *Metody sotsial'no-ekonomicheskogo prognozirovaniya* [Methods of socio-economic forecasting]. Moscow: National Training Foundation Publ., 2003. 395 p.
9. Mashunin Yu. K. *Razrabotka upravlencheskogo resheniya* [Development of management solutions]. Vladivostok: Far Eastern Federal Univ. Publ., 1999. 111 p.
10. Egorov A. I. *Osnovy teorii upravleniya* [Fundamentals of control theory]. Moscow: Fizmatlit Publ., 2004. 504 p.