DOI: https://doi.org/10.15688/jvolsu10.2017.4.2

УДК 681.3
ББК 32.973

МЕТОДИКА ИНВЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Светлана Сергеевна Козунова

Аспирант кафедры систем автоматизированного проектирования и поискового конструирования,
Волгоградский государственный технический университет
cad@vstu.ru
просп. им. Ленина, 28, 400005 г. Волгоград, Российская Федерация

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru, ba_benko@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассмотрен анализ подходов к инвестированию информационной безопасности (ИБ) организаций. Предложена методика инвестирования, описывающая возможности применения теории управления инвестициями в ИБ с процессами обеспечения ИБ организаций.

Ключевые слова: методика инвестирования, информационная безопасность, управление, предприятие, менеджмент информационной безопасности, информационные активы.

В основе построения системы информационной безопасности (СИБ) организации лежит инвестирование проектов обеспечения информационной безопасности (ПОИБ). Финансовый диапазон ИБ, который устанавливается руководством, редко подлежит увеличению. При принятии решения об эффективном инвестировании ПОИБ нужно применять методику, способную реализовать эффективное вложение в СИБ [6]. В исследовании [8] отмечено, что на предприятии задачи ИБ сводятся к корпоративной безопасности, поэтому специалист по безопасности должен быть бизнес-аналитиком. На практике политика инвестирования ИБ является либо частью общей политики инвестирования проектов предприятия, либо частной политикой системы менеджмента качества. Авторами [5] проанализированы подходы к оценке затрат на ИБ, результатом анализа явилось то, что ни один из подходов не является универсальным для достижения эффективности инвестиций в ИБ, а также не ориентированным на отечественные организации. В работе [5] исследована специфика российского подхода к оценке затрат в ИБ, согласно которой основными этапами являются: аудит ИБ, идентификация рисков, оценка рисков, определение допустимых уровней рисков. Согласно [4], менеджмент риска ИБ способствует: идентификации и оценке рисков, осознанию и информированию о вероятности и последствиях рисков, проведению регулярного мониторинга и пересмотра процесса менеджмента рисков. На основании [2–8] можно сделать вывод, что проектируемая методика должна соответствовать ГОСТ и бизнес-процессам предприятия.

I	Аудит информационной безопасности / Предпроектное обследование объекта защиты
II	Разработка проектов по обеспечению информационной безопасности и технического задания
III	Тестовые испытания разработанной системы и документирование результатов согласно принятой методике проведения тестовых испытаний
IV	Проведение коррекции проектов по обеспечению информационной безопасности
V	Ввод в эксплуатацию разработанной системы
VI	Эксплуатационное сопровождение внедрённой системы
VII	Разработка новых проектов по обеспечению информационной безопасности по истечении срока аттестации защищаемых объектов

Методика инвестирования информационной безопасности организации

В работе [4] процесс менеджмента риска ИБ представлен двумя основными составляющими: «коммутация риска» с процессами управления и «мониторинг и переоценка рисков». В статье [7] процесс управления инвестициями в ИБ представлен как «черный ящик». Входными сигналами являются: стоимость активов, затраты на ИБ, коэффициент дисконтирования. Выходными – прогнозирование ущербов, интегральный критерий эффективности, оптимизация затрат.

Предложенная авторами методика (рисунок) включает семь этапов. На первом этапе производится аудит ИБ или предпроектное обследование объектов защиты, результатом работ данного этапа является формирование направлений ИБ (классификация задач обеспечения ИБ) и определение требований по ИБ. На втором этапе определяются сроки и этапы работ по ПОИБ, наем лицензиатов в области обеспечения ИБ (по необходимости), прием на работы специалистов или инженеров ИБ (в случае отсутствия специализированных штатных сотрудников). На третьем этапе выбирается методика проведения тестовых испытаний, проводится тестирование разработанной системы защиты (СЗ), осуществляется развертывание пилот-проекта, результаты тестирований документируются. На четвертом этапе производится согласование результатов тестирований и в случае необходимости вносятся изменения в ПОИБ. Пятый этап включает в себя внедрение разработанной СЗ и подготовку итогового пакета документов. Шестой этап включает: администрирование и мониторинг СЗ, техническую поддержку пользователей, проведение контрольных мероприятий. Заключительным этапом является разработка нового ПОИБ. Таким образом, предложенная методика (см. рисунок) отображает процессы ИБ и процедуры инвестирования. Характеристики инвестирования ИБ могут быть получены при помощи использования какой-либо модели, например, повышающей эффективность инвестиций в ИБ предприятия [6], или подходов, о которых говорилось выше. В работе [1] говорится о ценности информационных активов (ИА). Оценку ценности ИА необходимо проводить на первом этапе. В статье [2] предложена оценка значимости ИА. Оценку информационных рисков и рисков инвестирования ИБ необходимо проводить на втором и четвертом этапах.

Методика инвестирования ИБ, предложенная авторами статьи, содержит структуру, описывающую возможности применения теории управления инвестициями в ИБ, и топологию взаимодействия процедур инвестирования с процессами обеспечения ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Атаманов, Г. А. О цене и ценности информации / Г. А. Атаманов // Защита информации. Инсайд. – 2016. – № 6. – С. 19–21.

2. Бабенко, А. А. Модель оценки и прогнозирования рисков инвестирования информационной безопасности промышленных предприятий / А. А. Бабенко, С. С. Козунова // Научный результат. Серия: Информационные технологии : Сетевой научно-практический журнал. – 2016. – Т. 1, № 4. – С. 29–35.

3. ГОСТ Р 54869-2011 Проектный менеджмент. Требования к управлению проектом. – Введ. 2011–12–22. – М. : Стандартинформ, 2011. – 14 с.

4. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 2011–12–01. – М. : Стандартинформ, 2011. – 51 с.

5. Жаринова, С. С. Модель эффективности инвестиций в информационную безопасность предприятия / С. С. Жаринова, А. А. Бабенко // Моделирование экономических процессов современной России: отчет о научно-исследовательской работе. В 5 ч. Ч. 4. Разработка микроэкономических моделей. – Волгоград : Волгогр. науч. изд-во, 2014. – С. 88–112.

6. Жаринова, С. С. Повышение эффективности инвестиций в информационную безопасность предприятия / С. С. Жаринова, А. А. Бабенко // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства : материалы III Всерос. науч-практ. конф. (г. Волгоград, 24–25 апр. 2014 г.). – Волгоград : Изд-во ВолГУ, 2014. – С. 119–123.

7. Козунова, С. С. Автоматизированная система управления инвестициями в информационную безопасность предприятия / С. С. Козунова // XXI Региональная конф. молодых исследователей Волгоградской области. – Волгоград, 2016. – С. 134–136.

8. Савельев, М. Перекосы сознания «ИБшника» / М. Савельев // Безопасность деловой информации. – 2015. – № 9. – С. 41–43.

REFERENCES

1. Atamanov G.A. O tsene i tsennosti informatsii [About the Price and Value of Information]. *Zashchita informatsii. Inside*, 2016, no. 6, pp. 19-21.

2. Babenko A.A., Kozunova S.S. Model otsenki i prognozirovaniya riskov investirovaniya informatsionnoy bezopasnosti promyshlennykh predpriyatiy [Model of Assessment and Forecasting of Investment Risks of Information Security of Industrial Enterprises]. *Nauchnyy rezultat. Seriya: Informatsionnye tekhnologii : Setevoy nauchno-prakticheskiy zhurnal*, 2016, vol. 1, no. 4, pp. 29-35.

3. *GOST R 54869-2011 Proektnyy menedzhment. Trebovaniya k upravleniyu proektom. Vved. 2011–12–22* [GOST R 54869-2011 Project Management. Requirements to Project Management. Adopted on December 22, 2011]. Moscow, Standartinform Publ., 2011. 14 p.

4. *GOST R ISO/MEK 27005-2010 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti. Vved. 2011–12–01* [GOST R ISO/MEK 27005-2010 Information Technology. Methods and Means of Security. Management of Information Security Risk. Adopted on December 1, 2011]. Moscow, Standartinform Publ., 2011. 51 p.

5. Zharinova S.S., Babenko A.A. Model effektivnosti investitsiy v informatsionnuyu bezopasnost predpriyatiya [Model of Investments Efficiency in Information Security of the Enterprise]. *Modelirovanie ekonomicheskikh protsessov sovremennoy Rossii: otchet o nauchno-issledovatelskoy rabote. V 5 ch. Ch. 4. Razrabotka mikroekonomicheskikh modeley* [Modeling of Modern Russia' Economic Processes: Report on Scientific and Research Work. In 5 Parts. Part 4]. Volgograd, Volgogradskoe nauchnoe izd-vo, 2014, pp. 88-112.

6. Zharinova S.S., Babenko A.A. Povyshenie effektivnosti investitsiy v informatsionnuyu bezopasnost predpriyatiya [Improving the Efficiency of Investments in Information Security of the Enterprise]. *Aktualnye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: materialy III Vseros. nauch-prakt. konf. (g. Volgograd, 24–25 apr. 2014 g.)* [Urgent Issues of Regional Information Security in the Context of Information Space Globalization: Proceedings of the 3rd All-Russian Research and Practice Conference (Volgograd, April 24-25, 2014)]. Volgograd, Izd-vo VolGU, 2014, pp. 119-123.

7. Kozunova S.S. Avtomatizirovannaya sistema upravleniya investitsiyami v informatsionnuyu bezopasnost predpriyatiya [Automated System of Investment Management in Information Security of the Enterprise]. *XXI Regionalnaya konf. molodykh issledovateley Volgogradskoy oblasti* [21st Regional Conference of Young Researchers of the Volgograd Region]. Volgograd, 2016, pp. 134-136.

8. Savelyev M. Perekosy soznaniya «IBshnika» [The Distortions of Consciousness in Information Security Specialist]. *Bezopasnost delovoy informatsii*, 2015, no. 9, pp. 41-43.

THE TECHNIQUE OF INVESTMENT IN ENTERPRISE'S INFORMATION SECURITY

Svetlana Sergeevna Kozunova

Postgraduate Student, Department of Computer-Aided Design and Search Design,
Volgograd State Technical University
cad@vstu.ru
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Aleksey Aleksandrovich Babenko

Candidate of Pedagogical Sciences, Associate Professor,
Department of Information Security,
Volgograd State University
infsec@volsu.ru, ba_benko@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The paper analyzes the approaches to investment in enterprise's information security (IS). The authors propose the investment technique that describes the possibilities of applying the theory of investment management in the sphere of IS to the processes of providing IS to enterprises.

Investment in information security projects is the key factor of building an efficient information security system of the enterprise. The efficiency of investment depends on the choice of a technique that would ensure the high level of information security. In an enterprise, information security tasks are reduced to corporate security, so a security specialist must be a business analyst. In practice, the investment policy in the sphere of information security is either a part of the overall investment policy of the enterprise projects or a private policy of the quality management system.

The proposed technique reflects the processes of information security and investment procedures. Characteristics of information security investments can be obtained through the use of any model, for example, improving the efficiency of investments in information security of the enterprise.

Key words: investment technique, information security, management, enterprise, information security management, information assets.