

ВНЕДРЕНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТЬ ОРГАНИЗАЦИЙ НАЦИОНАЛЬНОЙ ЭНЕРГЕТИКИ

С. Ю. Воробьев¹⁾, Е. А. Ханчевский²⁾

¹⁾ *заведующий сектором информационной безопасности, Научно-исследовательское и проектно-изыскательское республиканское унитарное предприятие «Белэнергосетьпроект», г. Минск, Беларусь, s.varabyou@besp.by*

²⁾ *начальник отдела информационных технологий, Научно-исследовательское и проектно-изыскательское республиканское унитарное предприятие «Белэнергосетьпроект», г. Минск, Беларусь, zh@besp.by*

Цифровизация белорусской экономики ставит перед организациями энергетической отрасли (далее – Организации) задачи обеспечения надлежащего уровня информационной безопасности (далее – ИБ). Внедрение системы менеджмента информационной безопасности (далее – СМИБ) в деятельность Организаций позволит выявить и минимизировать риски ИБ и обеспечить соблюдение нормативных и договорных требований в части обеспечения защиты информации.

Ключевые слова: энергетика; информационная безопасность; система менеджмента; СМИБ; ISO/IEC 27001.

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM IN THE ACTIVITIES OF NATIONAL ENERGY ORGANIZATIONS

S. Yu. Vorobyov¹⁾, E. A. Khanchevsky²⁾

¹⁾ *head of the information security sector, Scientific research and design and survey republican unitary enterprise «Belenergoseiproekt», Minsk, Belarus, s.varabyou@besp.by*

²⁾ *head of the information technology department, Scientific research and design and survey republican unitary enterprise «Belenergoseiproekt», Minsk, Belarus, zh@besp.by*

The digitalization of the Belarusian economy sets the task for energy industry organizations to ensure an appropriate level of information security. The introduction of an information security management system into the activities of Organizations will help identify and minimize information security risks, and ensure compliance with regulatory and contractual requirements regarding information security.

Keywords: energy; information security; management system; ISMS; ISO/IEC 27001.

Энергетика, как одна из ведущих отраслей белорусской экономики, наравне с последней переживает процесс цифровизации, что ставит перед руководителями Организаций ответственные задачи по непосредственному управлению процессами ИБ.

ИБ объектов энергетики исследовалась в работах С. Ю. Воробьева, Е. А. Ханчевского, А. И. Белоуса, В. А. Северина [1–3]. Повышение состояния защищенности информационных активов предприятий и организаций путем создания и внедрения в их деятельность СМИБ проанализировано П. А. Лонцих, М. Д. Хвистиком [4–5]. В настоящее время отсутствует исследование, посвященное актуальности внедрения СМИБ в деятельность Организаций.

Целью статьи состоит в актуальности внедрения СМИБ в деятельность Организаций для повышения эффективности процессов ИБ.

Набором общепризнанных международным сообществом требований и лучших практик, предъявляемых к СМИБ, является серия стандартов ISO/IEC 270xx, принятая Международной организацией по стандартизации ISO (International Organization for Standardization). После проведения мероприятий по переводу и терминологической адаптации Государственным комитетом по стандартизации Республики Беларусь данные стандарты были введены в действие (по содержанию и смысловой нагрузке они полностью идентичны стандартам ISO). В национальной системе стандартизации действуют следующие из них:

СТБ 27000 представляет собой общий обзор СМИБ и терминологическую базу [6];

СТБ 27001 – основной стандарт, устанавливающий требования к разработке, внедрению, поддержанию и постоянному улучшению СМИБ в контексте организации [7];

СТБ 27002 предназначен для использования в качестве углубленного справочного материала при определении и внедрении средств управления для обработки рисков ИБ в СМИБ [8];

СТБ 27003 описывает процессный подход по реализации проекта СМИБ [9];

СТБ 27004 – руководство по разработке и проведению процесса измерения внедренной СМИБ [10];

СТБ 27005 описывает процесс менеджмента рисков ИБ [11].

Внедрение СМИБ в деятельность Организаций позволит вовлечь высший менеджмент в непосредственное участие управления процессами ИБ, идентифицировать и минимизировать риски ИБ, продемонстрировать контрагентам, органам государственного управления, контрольным и надзорным инстанциям приверженность выполнения нормативных и договорных требований в части ИБ, четко разделить обязанности и полномочия в сфере защиты информации, привить собственным сотрудникам культуру ИБ, укрепить деловую репутацию, и, как следствие, увеличить собственные доходы и инвестиционную привлекательность.

Библиографические ссылки

1. Воробьев С. Ю., Ханчевский Е. А. Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности // Энергетическая стратегия. 2024. Т. 102, № 6. С. 33–36.
2. Белоус А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. М. : Вологда : Инфра-Инженерия, 2020. 644 с.
3. Северин В. А. Проблемы правового регулирования и методического обеспечения защиты информации в организациях ТЭК // Проблемы экономики и юридической практики. 2022. Т. 18, № 2. С. 96–103.
4. Лонцих П. А., Сафонова О. М. Методика создания и внедрение системы менеджмента информационной безопасности на промышленном предприятии // Системы. Методы. Технологии. 2020. № 4(48). С. 80–87.
5. Хвистик М. Д., Серенков П. С. Разработка и внедрение системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013 // Приборостроение-2021 : Материалы 14-й Международной научно-технической конференции, Минск, 17–19 ноября 2021 года. Минск : Белорусский национальный технический университет, 2021. С. 242–243.
6. Информационные технологии. Методы обеспечения безопасности. Общий обзор и словарь : СТБ ISO/IEC 27000-2024. Введ. 25.10.24 (с отменой на территории РБ СТБ ISO/IEC 27000-2012). Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. 23 с.
7. Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования : СТБ ISO/IEC 27001-2024. Введ. 25.10.24 (с отменой на территории РБ СТБ ISO/IEC 27001-2016). Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. 19 с.

8. Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью : СТБ ISO/IEC 27002-2024. Введ. 25.10.24 (с отменой на территории РБ СТБ ISO/IEC 27002-2012). Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. 132 с.

9. Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности : СТБ ISO/IEC 27003-2014. Введ. 14.08.14. Минск : Научн.-исслед. ин-т техн. защиты информации. 59 с.

10. Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения : СТБ ISO/IEC 27004-2014. Введ. 14.08.14. Минск : Научн.-исслед. ин-т техн. защиты информации. 53 с.

11. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по менеджменту рисков информационной безопасности : СТБ ISO/IEC 27005-2024. Введ. 25.10.24 (с отменой на территории РБ СТБ ISO/IEC 27005-2012). Минск : Белорус. гос. ин-т стандартизации и сертификации, 2024. 56 с.