УДК 004.056.5:006.89

РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ СТБ ISO/IEC 27001-2024 В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

С.Ю. Воробьёв, Е.А. Ханчевский

Научно-исследовательское и проектно-изыскательское республиканское унитарное предприятие «Белэнергосетьпроект», г. Минск, Республика Беларусь

Аннотация. Процессы цифровой трансформации энергетической отрасли служат триггером для осуществления комплекса мероприятий по защите информации, обрабатываемой в информационных системах организаций и предприятий белорусской энергетики. Вместе с тем вопросы эффективности результатов внедрения требований стандарта СТБ ISO/IEC 27001-2024 в операционную деятельность последних остаются практически неизученными как на уровне научной среды, так и работников производственной сферы. В статье приведен кейс по внедрению системы менеджмента информационной безопасности в деятельность одного из предприятий, структурно входящего в ГПО «Белэнерго» Министерства энергетики Республики Беларусь с интерпретацией полученных результатов.

Ключевые слова: энергетика; информационная безопасность; защита информации; системы менеджмента; стандарты; сертификация; кибербезопасность, риски информационной безопасности; 27001.

IMPLEMENTATION OF STB ISO/IEC 27001-2024 REQUIREMENTS IN THE ACTIVITIES OF AN ENERGY INDUSTRY ENTERPRISE

S.Yu. Vorobyov, E.A. Khanchevsky

Belenergosetproekt, a research and development and design and survey republican unitary enterprise, Minsk, Republic of Belarus

Abstract. The digital transformation of the energy sector is triggering a series of measures to protect information processed in the information systems of Belarusian energy

organizations and enterprises. However, the effectiveness of implementing the requirements of the STB ISO/IEC 27001-2024 standard in the operations of these organizations remains largely unexplored, both by the scientific community and by industry professionals. This article presents a case study of implementing an information security management system at one enterprise, part of the Belenergo State Production Association of the Ministry of Energy of the Republic of Belarus, and an interpretation of the results.
Keywords: energy; information security; information protection; management systems; standards; certification; cybersecurity; information security risks; 27001.

Введение

Энергетика по праву относится к системообразующим компонентам национальной экономики и перманентно подвержена всем протекающим в ней процессам, в том числе цифровизации. Уязвимой точкой последней является восприимчивость к кибератакам, что ставит актуальную задачу по эффективному управлению процессами информационной безопасности (ИБ) в производственной деятельности организаций и предприятий.

Проблематика ИБ на объектах энергетики исследовалась белорусскими и российскими авторами С. Ю. Воробьёвым, А. И. Белоусом, И. Н. Колоском [1–3]. Эффективность внедрения системы менеджмента ИБ (далее – СМИБ) в операционную деятельность организаций анализировалась в работах А. А. Кайсаровой, А. Т. Касымбека П. А. Лонцих [4–6].

Вместе с тем в настоящее время отсутствуют исследования, посвященные изучению эффективности от внедрения СМИБ в производственную деятельность организаций и предприятий энергетической отрасли. Целью работы является рассмотрение практического кейса по внедрению СМИБ в деятельность одного из предприятий, структурно входящего в ГПО «Белэнерго» Министерства энергетики Республики Беларусь (далее – Предприятие), интерпретация полученных от его реализации результатов, возможность их имплементации в производственную деятельность белорусских энергетических организаций и предприятий.

Основная часть

Серия стандартов ISO/IEC 270xx, принятая Международной организацией по стандартизации ISO (International Organization for Standardization), представляет собой набор общепризнанных лучших практик и требований, предъявляемых к СМИБ. После осуществления перевода и терминологической адаптации Государственным комитетом по стандартизации Республики Беларусь данные технические нормативные правовые акты) были введены в действие на территории Республики Беларусь (по содержанию и смысловой нагрузке они полностью идентичны стандартам ISO).

Организации белорусской энергетической системы вынуждены проводить комплекс мероприятий организационного, правового и технического характера для защиты самого ценного информационного общества: информации. Одним из направлений повышения состояния защищенности информационных активов является разработка и внедрение СМИБ в соответствии с требованиями СТБ 27001, общепринятого набора мировых лучших практик в сфере защиты информации. Интеграция СМИБ в практическую деятельность любой организации вне зависимости от рода деятельности, принадлежности к государственному или частному сектору, численности позволяет 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 требований ИБ, четко разделить обязанности и полномочия в сфере защиты информации, привить собственным работникам культуру защиты информации, укрепить деловую репутацию, и, соответственно, увеличить собственные доходы и инвестиционную привлекательность.

Подтверждение соответствия СМИБ требованиям СТБ 27001, подтвержденное сертификатом в Национальной системе подтверждения соответствия, ставит перед Предприятием очередную амбициозную задачу: осуществление мероприятий на получение лицензии по проектированию, созданию и аудиту систем информационной безопасности критически важных объектов информатизации.

Заключение

СМИБ не является панацеей от хищения конфиденциальной информации, коммерческого шпионажа, или кибератак на АЭС, но проведение мероприятий согласно методологии, основанной на рискориентированном подходе, описанной в СТБ 27001 позволит повысить защищенность самого ценного ресурса XXI века: информации.

Список использованных источников

1. Воробьёв, С. Ю. Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности / С. Ю. Воробьёв, Е. А. Ханчевский // Энергетическая стратегия. – 2024. – Т. 102, № 6. – С. 33–36.

2. Белоус, А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А.И. Белоус. – Москва ; Вологда : Инфра-Инженерия, 2020. – 644 с.

3. Анализ кибербезопасности объектов энергетики с учетом механизма и кинетики нежелательных процессов / И. Н. Колосок, Е. С. Коркина // Энергетик. – 2024. – № 2. – С. 3–8.

4. Внедрение международного стандарта ИСО/МЭК 27001 – основа управления информационной безопасностью предприятия / А. А. Кайсарова, А. К. Тулекбаева, А. А. Токтабек [и др.] // Вестник науки Южного Казахстана. – 2018. – № 4 (4). – С. 103–106.

5. Касымбек, А. Т. Польза от внедрения международного стандарта ISO/IEC 27001 / А. Т. Касымбек // Евразийское Научное Объединение. – 2015. – Т. 1, № 2(2). – С. 52–53.

6. Лонцих, П. А. Методика создания и внедрение системы менеджмента информационной безопасности на промышленном предприятии / П. А. Лонцих, О. М. Сафонова // Системы. Методы. Технологии. – 2020. – № 4(48). – С. 80–87.

References

1. Vorobyov, S. Yu. Cyberattacks on Critical Energy Facilities as a Source of National Security Threats / S. Yu. Vorobyov, E. A. Khanchevsky // Energy Strategy. – 2024. – Vol. 102, No. 6. –P. 33–36.

2. Belous, A. I. Cybersecurity of Fuel and Energy Complex Facilities. Concepts, Methods, and Means of Support / A. I. Belous. – Moscow; Vologda: Infra-Engineering, 2020. – 644 p.

3. Analysis of Cybersecurity of Energy Facilities Taking into Account the Mechanism and Kinetics of Undesirable Processes / I. N. Kolosok, E. S. Korkina // Energetik. – 2024. – No. 2. – P. 3–8.

4. Implementation of the international standard ISO / IEC 27001 – the basis for enterprise information security management / A. A. Kaisarova, A. K. Tulekbaeva, A. A. Toktabek [et al.] // Bulletin of Science of South Kazakhstan. – 2018. – No. 4 (4). – P. 103–106.

5. Kasymbek, A. T. Benefits of implementing the international standard ISO / IEC 27001 / A. T. Kasymbek // Eurasian Scientific Association. – 2015. – Vol. 1, No. 2 (2). – P. 52–53.

6. Lontsikh, P. A. Methodology for the creation and implementation of an information security management system at an industrial enterprise / P. A. Lontsikh, O. M. Safonova // Systems. Methods. Technologies. – 2020. – No. 4 (48). – P. 80–87.

Сведения об авторах

Воробьёв С.Ю., магистр технических наук, заведующий сектором информационной безопасности отдела информационных технологий организации научно-исследовательского и проектно-изыскательского республиканского унитарного предприятия «Белэнергосетьпроект», s.varabyou@besp.by.

Ханчевский Е.А., начальник отдела информационных технологий организации научно-исследовательского и проектно-изыскательского республиканского унитарного предприятия «Белэнергосетьпроект», zh@besp.by.

Information about the authors

Vorobyov S.Yu., Master of Engineering Sciences, Head of the Information Security Sector, Information Technology Department, Research and Design and Survey Organization, Republican Unitary Enterprise «Belenergosetproekt», s.varabyou@besp.by.

Khanchevsky E.A., Head of the Information Technology Department, Research and Design and Survey Organization, Republican Unitary Enterprise «Belenergosetproekt», zh@besp.by.