УДК 338.22:621.3

Система экономической безопасности предприятий электроэнергетики: принципы построения и функционирования

А.В. Бозина
студент 2 курса магистратуры НИЯУ МИФИ, Москва
Email: bozinauser@gmail.com
А.И. Нечаева
студент 2 курса магистратуры НИЯУ МИФИ, Москва
Email: nastia_novosib@mail.ru
П.Ю. Леонов
к.э.н., доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва
Email: PYLeonov@mephi.ru

Аннотация: *Статья исследует систему экономической безопасности предприятий электроэнергетики на примере ПАО «Интер РАО», раскрывая ключевые принципы её построения: законность, комплексность, превентивность, разграничение доступа и другие. Рассмотрены функциональные составляющие (финансовая, информационная, экологическая безопасность) и практические механизмы их реализации в условиях санкций и цифровых угроз. Особое внимание уделено анализу соответствия деятельности компании международным стандартам и российскому законодательству.*

Ключевые слова: *экономическая безопасность, электроэнергетика, ПАО «Интер РАО», риск-менеджмент, кибербезопасность, санкционные риски, критическая инфраструктура, законодательное регулирование*

The system of economic security of electric power industry enterprises: principles of construction and functioning

A.V. Bozina
2nd year master’s student at NRNU MEPhI, Moscow
Email: bozinauser@gmail.com
A.I. Nechaeva
2nd year master’s student at NRNU MEPhI, Moscow
Email: nastia_novosib@mail.ru
P.Y. Leonov
Ph.D., Associate Professor department of financial monitoring
NRNU MEPhI, Moscow
Email: PYLeonov@mephi.ru

Abstract: *The article examines the economic security system of electric power enterprises using PJSC "Inter RAO" as a case study, outlining key principles of its construction: legality, comprehensiveness, preventive measures, access control, and others. It explores functional components (financial, information, environmental security) and practical mechanisms for their implementation under sanctions and digital threats. Special attention is given to analyzing the company's compliance with international standards and Russian legislation.*

Keywords: *economic security, electric power industry, PJSC "Inter RAO", risk management, cybersecurity, sanction risks, critical infrastructure, legislative regulation*

Электроэнергетика – отрасль энергетики, которая включает в себя производство, передачу и сбыт электрической энергии. Данная отрасль обеспечивает электричество для промышленных предприятий, домашних потребителей, транспортных средств и других сфер. Электроэнергетика является одной из стратегически важных отраслей экономики, которая определяется тем, что она обеспечивает функционирование всех секторов экономики, является инфраструктурной основой цифровой экономики.

Прежде чем перейти к рассмотрению системы экономической безопасности в сфере электроэнергетики, необходимо ознакомиться с особенностями отрасли. Рассмотрим технологические особенности и некоторые важные влияющие экономические факторы. К технологическим особенностям отрасли относятся: непрерывность процессов производства и потребления энергии, то есть электростанции должны вырабатывать мощность всегда; необходимо всегда иметь резервы, то есть делать резервы генерирующих мощностей, пропускной способности сетей и запасов топлива; динамичность производственных процессов (ввиду того, что нагрузка на энергосистемы постоянно меняется, что требует создания специального маневренного оборудования). Экономическими факторами электроэнергетики являются – сложность и особые условия работы оборудования, влияние режима потребления на производство (объемы выработки зависят от графика нагрузки потребителей, сезонности и т.д.) Также необходимо отметить сильную зависимость от природных и климатических факторов [8]. Следовательно, необходимо отметить, что важность отрасли определяется тем, что она обеспечивает энергетическую безопасность государства, а также устойчивое развитие всех секторов народного хозяйства. В современных условиях предприятия в сфере электроэнергетики сталкиваются с большим количеством различных угроз, некоторые из них будут описаны далее:

- Киберугрозы
- Технологические риски
- Финансовые риски
- Внешние вызовы

– Экологические риски

Для минимизации возникновения данных угроз и их ущерба, предприятиям необходимо создать систему экономической безопасности.

Под системой экономической безопасности подразумевается совокупность взаимосвязанных элементов, направленных на обеспечение защиты экономических интересов организации, ее устойчивого развития в условиях воздействия внутренних и внешних угроз. Необходимо отметить, что это не набор случайных мер, а целенаправленно организованный комплекс действий.

Система экономической безопасности предприятия строится на определенных принципах:

1. Законность

Все меры и действия в рамках системы экономической безопасности должны соответствовать законодательству РФ. Использование методов, нарушающих права и свободы граждан, а также наносящих ущерб окружающей среды, недопустимо.

2. Комплексность и системность

Все сферы деятельности предприятия должны быть охвачены системой экономической безопасности (финансовая, информационная, технологическая, правовая, кадровая, производственная, экологическая).

3. Пропорциональность (экономическая целесообразность)

Затраты на обеспечение экономической безопасности должны быть соразмерны уровню угроз и потенциальному ущербу.

4. Непрерывность и динамичность

Система экономической безопасности предприятия должна функционировать в непрерывном режиме, обеспечивая постоянный мониторинг угроз и оперативное реагирование на возникающие, в процессе деятельности, риски. Также необходимо проводить анализ эффективности СЭБ регулярно и, при необходимости, вносить корректировки.

5. Централизация и децентрализация

Централизация в экономической безопасности предприятия - это сосредоточение управления рисками, контроля и принятия ключевых решений на верхнем уровне руководства для обеспечения единой защитной стратегии. Децентрализация представляет собой делегирование полномочий по структурным подразделениям, что повышает оперативность реагирования на локальные угрозы и адаптивность бизнеса. Оптимальное сочетание этих подходов позволяет организации оставаться гибкими в меняющихся условиях.

6. Разграничение доступа и конфиденциальность

Данный принцип предполагает строгое регулирование прав доступа, что минимизирует внутренние и внешние угрозы утечки информации.

7. Взаимодействие и сотрудничество

Данный принцип предполагает согласованность действий между отделами, сторонними организациями и контролирующими органами. Это необходимо для оперативного обнаружения потенциальных рисков, обмена важными данными и создания всесторонней системы защиты бизнеса.

8. Превентивность

Превентивность обеспечивает экономическую безопасность предприятия за счёт системного анализа рисков и внедрения защитных механизмов на ранних стадиях, что снижает вероятность возникновения критических инцидентов.

9. Профессионализм

Как принцип экономической безопасности, профессионализм подразумевает наличие у сотрудников специальных знаний, компетенций, необходимых для эффективного выявления и нейтрализации угроз в постоянно меняющихся условиях бизнес-среды.

10. Ответственность

Обеспечивает эффективную систему экономической безопасности за счет закрепления зон контроля за каждым участником бизнес-процессов и механизмов оценки их вклада в защиту активов предприятия [6].

После рассмотрения принципов, на которых строится система экономической безопасности, перейдем к задачам. Основная задача создания системы экономической безопасности организации состоит в поддержании ее устойчивой деятельности и достижении наивысшей производительности в настоящем времени, а также минимизации ущерба как от внешних, так и внутренних угроз.

Экономическая безопасность состоит из функциональных составляющих, представленных на рисунке 1.

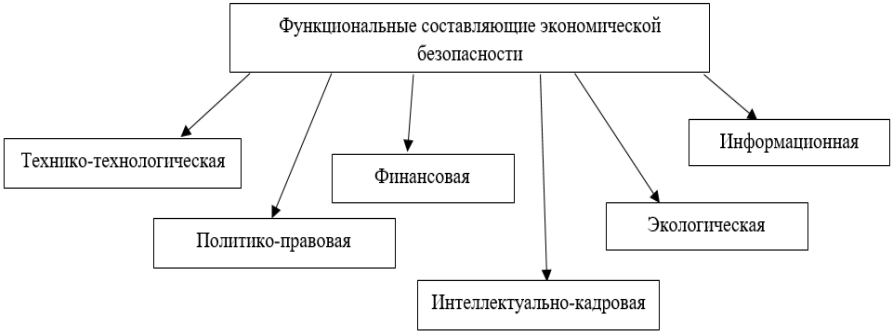

Рисунок 10 – Функциональные составляющие экономической безопасности

Для более глубокого понимания необходимо рассмотреть каждый аспект детальнее.

Финансовая безопасность организации является ключевым элементом его экономической безопасности. Она отражает уровень защищенности финансовых активов и экономических интересов компании, возникающих

как внутри, так и за ее пределами, что обеспечивает ее устойчивое развитие и функционирование. Важным аспектом является минимизация финансовых рисков, связанных с дебиторской и кредиторской задолженностью. [4].

Под экологической безопасностью понимается защита от разрушительного воздействия природных, техногенных, факторов хозяйственной деятельности организация, предотвращение или минимизация вреда окружающей среде от деятельности предприятия. Компании заботятся об экологии, соблюдая природоохранные нормы, снижая вредные выбросы и внедряя "зелёные" технологии, чтобы вести бизнес ответственно и устойчиво.

Технико-технологическая составляющая экономической безопасности говорит о том, что организации должны так формировать и применять оборудование, техническую базу и основных средств производства, а также бизнес-процессы и технологии, чтобы они способствовали росту уровня конкурентоспособности организации.

В контексте экономической безопасности предприятия, информационная составляющая играет ключевую роль в обеспечении сохранности конфиденциальных сведений, коммерческой тайны и цифровых ресурсов. Это достигается путем противодействия как внутренним, так и внешним рискам, таким как кибератаки, несанкционированное раскрытие данных и недобросовестная конкуренция в виде промышленного шпионажа.

Политико-правовой аспект включает в себя соблюдение нормативной базы, защищая свои имущественные права. Регулярное взаимодействие с государственными учреждениями и корректировка деятельности в соответствие с изменениями в нормативных актах позволяют сократить вероятность возникновения правовых проблем и сложностей в административных процедурах, что способствует укреплению устойчивости предпринимательской деятельности.

Интеллектуально-кадровая составляющая экономической безопасности включает в себя наличие квалифицированных кадров компании. Для чего организация должна создавать условия для постоянного профессионального роста и развития. Эффективная система обучения и мотивации помогает формировать высококвалифицированную команду [4].

Теоретические концепции нуждаются в проверке на практике. Рассмотрим крупную компанию электроэнергетической отрасти – ПАО «Интер РАО», проанализируем насколько компания соблюдает принципы построения системы экономической безопасности.

ПАО «Интер РАО» - российская энергетическая компания с государственным участием, специализирующаяся на экспорте-импорте электроэнергии, генерации и распределении энергоресурсов. Входит в число крупнейших игроков энергорынка Евразии, управляя активами в России и за рубежом.

Для начала рассмотрим соблюдение такого принципа построения системы экономической безопасности, как законность. ПАО «Интер РАО» может похвастаться строгим соблюдением требований российского и международного права. Это выражается в соблюдении таких федеральных законов как: №35-ФЗ "Об электроэнергетике"; №273-ФЗ "О противодействии коррупции"; №135-ФЗ "О защите конкуренции"; № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма". Также, необходимо отметить, что ПАО «Интер РАО» проходит ежегодный аудит финансовой отчетности, что говорит о достоверности финансовой отчетности, об отсутствии финансовых махинаций и отмывании доходов.

Принцип комплексности и системности экономической безопасности в ПАО «Интер РАО» реализуется через взаимосвязанную систему защиты всех направлений деятельности: от финансовых рисков (контроль валютных операций и антисанкционная политика) и информационной безопасности (защита данных и киберзащита критической инфраструктуры) до физической охраны объектов и кадровой безопасности. Компания использует единый центр управления рисками, который координирует взаимодействие службы безопасности, финансового контроля, юридического департамента и IT-защиты, объединяя данные о финансовых потоках, техническом состоянии объектов, кадровых изменениях и внешних угрозах в автоматизированной системе мониторинга. Такой подход позволяет одновременно анализировать все аспекты при выходе на новые рынки (проверка контрагентов, адаптация IT-систем, оценка политических рисков) и обеспечивать защиту критической инфраструктуры (физическая охрана, киберзащита SCADA-систем, подготовка персонала), что снижает издержки, ускоряет выявление взаимосвязанных угроз и повышает устойчивость компании в условиях санкций и колебаний энергорынков.

Принцип разграничения доступа и конфиденциальности в ПАО «Интер РАО» реализуется через многоуровневую систему защиты критически важной информации, включающую строгую классификацию данных (коммерческая тайна, персональные данные, техническая документация) и дифференцированный доступ сотрудников в зависимости от их должностных обязанностей. Компания использует современные решения для контроля доступа (электронные пропуска, биометрическая идентификация, системы DLP), шифрование корпоративной переписки и защищенные каналы передачи данных, что особенно важно при работе с международными контрагентами и в условиях усиленных киберугроз. Внедрение ролевой модели доступа к информационным системам (ERP, CRM, SCADA) и регулярный аудит прав пользователей позволяют минимизировать риски внутренних утечек, обеспечивая при этом бесперебойную работу энергетической инфраструктуры и соблюдение

требований как российского законодательства (152-ФЗ, 98-ФЗ), так и международных стандартов информационной безопасности.

Принцип превентивности в системе экономической безопасности ПАО «Интер РАО» реализуется через комплекс упреждающих мер, направленных на прогнозирование и нейтрализацию потенциальных угроз до их реализации. Компания использует современные системы риск-менеджмента, включая регулярный мониторинг санкционных рисков (в соответствии с методиками Минэкономразвития РФ) и стресс-тестирование финансовой устойчивости по стандартам Базель III. Особое внимание уделяется защите критической инфраструктуры через обязательное проведение киберучений на энергообъектах (согласно требованиям ФСТЭК России) и заблаговременную разработку альтернативных логистических схем поставок оборудования (в условиях импортозамещения). Аналитический центр безопасности компании ежеквартально обновляет матрицы угроз с учетом изменений геополитической ситуации, что позволяет заранее адаптировать бизнес-процессы. Внедрение системы раннего предупреждения о мошеннических схемах (на базе технологий Big Data) и обязательный compliance-аудит всех международных контрактов обеспечивают минимизацию потенциальных потерь при работе на глобальных энергетических рынках.

Список использованных источников:

1. Федеральный закон от 07.08.2001 № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

2. Иванов А.В. Экономическая безопасность компаний ТЭК: современные вызовы и решения. – М.: Энергоиздат, 2022

3. Петрова С.К. "Киберриски в электроэнергетике: международный опыт защиты"//Вопросы экономической безопасности – 2023– № 4–С.45–52

4. Лапин В.Н. Экономическая безопасность предприятия. — М.: ИНФРА-М, 2019.

5. Бобылев С.Н., Соловьёва С.В. Экономическая безопасность предприятия. — М.: КноРус, 2022.

6. Петрова, С.К. "Методологические основы построения СЭБ в условиях цифровизации" // Вопросы кибербезопасности. – 2022. – №3(12). – С. 18-25.

7. Губанова Е. Н. Экономическая безопасность предприятия: учебное пособие. — М.: Инфра-М, 2020.

8. Королев В. Г. «Современные особенности и состояние электроэнергетической отрасли РФ» // 2020.

9. Официальный сайт ПАО «Интер РАО» [Электронный ресурс]. – Режим доступа: https://www.interrao.ru/?ysclid=mawt96ocdv191844031

10. Годовой отчет ПАО «Интер РАО» за 2023 год [Электронный ресурс]. – Режим доступа: interrao.ru/upload/InterRAO_AR2023_RUS_2.pdf