Научная статья
УДК 65.012.8
DOI: 10.25683/VOLBI.2024.69.1136

Alexander Aleksandrovich Lomeiko
Postgraduate of the Department of Management,
field of training 5.2.6 — Management,
Peoples' Friendship University of Russia
named after Patrice Lumumba
Moscow, Russian Federation
1142220832@rudn.ru

Александр Александрович Ломейко
аспирант кафедры менеджмента,
направление подготовки 5.2.6 — Менеджмент,
Российский университет дружбы народов
имени Патриса Лумумбы
Москва, Российская Федерация
1142220832@rudn.ru

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ БЕЗОПАСНОСТЬЮ НА ПРИМЕРЕ АО «МОСЭНЕРГОСБЫТ»

5.2.3 — Региональная и отраслевая экономика

Аннотация. *В статье рассматривается важнейшая роль комплексной системы управления корпоративной безопасностью. Статья посвящена актуальной проблеме совершенствования системы управления корпоративной безопасностью на примере крупной энергетической компании АО «Мосэнергосбыт». В условиях растущих киберугроз и возрастающей зависимости от критической инфраструктуры обеспечение корпоративной безопасности становится одним из приоритетных направлений для энергетических компаний. В работе проведен глубокий анализ существующих исследований в области корпоративной безопасности, выявлены основные тенденции и направления развития. Автор обосновывает необходимость повышения уровня корпоративной безопасности в энергетическом секторе, учитывая растущие угрозы и риски. На основе системного анализа выявлены ключевые угрозы и риски, характерные для данного сектора. Также выявлены такие аспекты, как оценка рисков, управление инцидентами, повышение осведомленности сотрудников и развитие корпоративной культуры безопасности.*

Ключевым результатом исследования является разработка модели, описывающей взаимосвязи между компонентами системы корпоративной безопасности и позволяющей оптимизировать процессы управления корпоративной безопасностью энергетической компании АО «Мосэнергосбыт». Данная модель позволяет оптимизировать процессы принятия решений, повысить эффективность реагирования на угрозы и обеспечить непрерывность бизнеса энергетических предприятий в современных условиях развития отраслевого сектора энергетического рынка России.

Проведенное исследование демонстрирует, что обеспечение корпоративной безопасности в энергетическом секторе является сложной и многогранной задачей, особенно для АО «Мосэнергосбыт». Однако благодаря применению современных технологий и системного подхода можно создать эффективную систему защиты, способную противостоять современным киберугрозам. Комплексный подход, включающий не только технические средства защиты, но и организационные меры, такие как обучение персонала и регулярные аудиты безопасности, позволяет создать многоуровневую систему защиты, способную минимизировать риски кибератак.

Ключевые слова: *корпоративная безопасность, кибербезопасность, система управления, АО «Мосэнергосбыт», безопасность, физическая безопасность, анализ рисков, управление инцидентами, непрерывность бизнеса, энергетические компании*

Для цитирования: Ломейко А. А. Совершенствование системы управления корпоративной безопасностью на примере АО «Мосэнергосбыт» // Бизнес. Образование. Право. 2024. № 4(69). С. 108—115. DOI: 10.25683/VOLBI.2024.69.1136.

Original article

IMPROVING THE CORPORATE SECURITY MANAGEMENT SYSTEM USING THE EXAMPLE OF MOSENERGOSBYT JSC

5.2.1 — Regional and sectoral economy

Abstract. *The article considers the most important role of an integrated corporate security management system. The article is devoted to the urgent problem of improving the corporate security management system on the example of a large energy company Mosenergosbyt JSC. In the context of growing cyber threats and increasing dependence on critical infrastructure, ensuring corporate security is becoming one of the priorities for energy companies. The paper provides an in-depth analysis of existing research in the field of corporate security, identifies its main trends and directions of development. The author substantiates the need to increase the level of corporate security in the energy sector, taking into account the growing threats and risks. Based on the system analysis, the key threats and risks specific to this sector are identified, as well as risk assessment, incident management, employee awareness raising and the development of a corporate safety culture.*

The key result of the research is the development of a model describing the relationships between the components of the corporate security system, which allows optimizing the corporate security management processes of the energy company Mosenergosbyt JSC. This model makes it possible to optimize decision-making processes, increase the effectiveness of responding to threats and ensure business continuity of energy enterprises in modern conditions of development of the industrial sector of the Russian energy market.

The conducted research demonstrates that ensuring corporate security in the energy sector is a complex and multifaceted

task, especially for the company Mosenergosbyt JSC. However, thanks to the use of modern technologies and a systematic approach, it is possible to create an effective protection system capable of resisting modern cyber threats. An integrated approach, which includes not only technical means of protection, but also organizational measures such as staff training and regular security audits, allows you to create a multi-level protection system capable of minimizing the risks of cyber-attacks.

Keywords: *corporate security, cybersecurity, management system, Mosenergosbyt JSC, security, physical security, risk analysis, incident management, business continuity, energy companies*

For citation: Lomeiko A. A. Improving the corporate security management system using the example of Mosenergosbyt JSC. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2024;4(69):108—115. DOI: 10.25683/VOLBI.2024.69.1136.

Введение

Актуальность. В современном мире, характеризующемся сложными взаимосвязями, обеспечение корпоративной безопасности приобретает первостепенное значение для предприятий, работающих в различных секторах. Энергетические компании, в частности, сталкиваются с особым набором препятствий из-за важного характера своей деятельности, что может иметь далеко идущие последствия как для самой компании, так и для широкой общественности.

Энергетический сектор является стержнем современного общества, предоставляя важнейшие услуги, которые лежат в основе экономического роста и социального благополучия. Обеспечение корпоративной безопасности энергетических предприятий является многогранным процессом, поскольку предполагает не только активное взаимодействие предприятия с внешней средой, но и наличие существенных внутренних противоречий между его участниками. Взаимодействие может иметь как положительные, так и отрицательные последствия, проявляясь в виде внешних вызовов, рисков и угроз. Утечка данных может привести к значительным потерям как на индивидуальном, так и на организационном уровнях. Поэтому частные лица и организации уделяют приоритетное внимание конфиденциальности данных в качестве первого шага в защите своей конфиденциальной информации. На индивидуальном уровне потеря данных может произойти через мобильные телефоны, электронную почту, платформы социальных сетей или при просмотре ненадежных веб-сайтов. С другой стороны, организации имеют дело с данными клиентов, и утечка данных может привести к существенным потерям.

Изученность проблемы. Проведенный анализ литературы показал спектр исследований в области корпоративной безопасности, сосредоточенных на различных аспектах этой проблемы. Авторы анализируют инвестиционные решения в сфере корпоративной безопасности, стратегические подходы к корпоративному управлению, влияние глобальных событий на корпоративную безопасность, роль корпоративной культуры, а также конкретные угрозы, такие как утечки данных и кадровые риски.

Х. Лю и Г. Рахимжанова исследуют стратегические подходы к корпоративному управлению, направленные на обеспечение экономической безопасности. Авторы подчеркивают важность долгосрочного планирования и адаптации к меняющимся внешним условиям [1].

S. Reka исследует стратегическую встроенность корпоративной безопасности в бизнес-процессы, а также анализирует, как корпоративная безопасность может быть интегрирована в стратегические планы компании [2].

T. Shyra с соавторами изучают развитие корпоративной безопасности в контексте противодействия угрозам для бизнеса. Авторы рассматривают различные виды угроз и предлагают меры по их минимизации [3].

J. Wu предлагает стратегию оценки безопасности корпоративных финансовых систем на основе методов *Data Mining* [4].

Российские авторы (Б. И. Истратов [5], Л. Н. Леванова [6], И. А. Никитина [7], Е. О. Соколова [8], А. В. Фролов [9], А. А. Якушкина [10]) фокусируются на различных аспектах корпоративной безопасности, включая стейкхолдерский подход, кадровую безопасность и защиту данных.

D. Baschung с соавторами изучают сложную взаимосвязь между инвестиционными решениями для сотрудников корпоративной безопасности (*CSO*) в сфере ИТ-безопасности [11]. Авторы оспаривают общепринятое экономическое предположение о том, что увеличение расходов на безопасность напрямую связано с усилением корпоративной безопасности. Авторы предлагают динамическую модель, в которой карьерный рост сотрудников, отвечающих за корпоративную безопасность, находится под существенным воздействием, как инвестиционных решений в сфере информационной безопасности, так и реальных кибератак, с которыми организации сталкиваются. В исследовании используется имитационная модель, основанная на модели Гордона—Лёба, для анализа динамики инвестиций, карьеры *CSO*, мобильности работы и эффективности мер кибербезопасности. Авторы пришли к выводу, что существует положительная корреляция между карьерой сотрудников и эффективностью мер корпоративной безопасности. Модель основана на данных о реальных нарушениях кибербезопасности с помощью моделирования процесса Монте-Карло. Исследование способствует пониманию принятых решений, с которыми сталкиваются руководители службы безопасности. Авторы подчеркивают потенциальное несоответствие между целями корпоративной безопасности и индивидуальными карьерными устремлениями. Моделируя взаимодействие инвестиций, репутации и карьерного роста, исследование предлагает понимание факторов, влияющих на поведение руководителей служб безопасности, и его последствий для корпоративной безопасности.

Н. Волосникова предлагает абстрактную модель корпоративной системы безопасности, которая может быть описана математически для оптимизации компонентов системы и повышения экономической эффективности [12]. Предлагаемая модель подчеркивает влияние информационной безопасности на общую стабильность системы. В ней признается, что информационная безопасность является критически важным элементом для обеспечения надлежащего функционирования корпоративной безопасности. Модель служит инструментом для оптимизации взаимодействия между различными элементами и оценки влияния информационной безопасности на эффективность всей корпоративной системы безопасности.

Н. Волосникова подчеркивает, что устойчивость является жизненно важным фактором поддержания надежной корпоративной системы безопасности. Устойчивая система

способна противостоять различным нарушениям, как внутренним, так и внешним. Способность возвращаться к стабильному состоянию после сбоев является ключевой характеристикой устойчивой системы.

E. P. Yıldız и O. Simsekler отметили, что, по данным Всемирного экономического форума о глобальных рисках за 2022 г., растет зависимость от технологических систем (после пандемии *COVID*-19), что приводит к резкому росту удаленной работы для большинства работников предприятий. Одновременно возросли угрозы кибербезопасности, т. к. в 2020 г. количество атак вредоносных программ и программ-вымогателей увеличилось на 358 и 435 % соответственно. Однако превентивные меры не были приняты, в первую очередь из-за нехватки специалистов по кибербезопасности и фрагментации структур управления. Результаты исследования глобального восприятия рисков за 2021—2022 гг. показали, что проблемы кибербезопасности занимают седьмое место в глобальном восприятии рисков, составляя 12,4 %. Более того, большинство участников считают, что текущее состояние усилий по снижению рисков в области трансграничных кибератак и дезинформации либо «еще не начато», либо «находится на ранних стадиях разработки», и указывает на отсутствие прогресса [13].

D. Milica утверждает, что корпоративная безопасность стала наиболее важной областью исследований после трагических событий 11 сентября 2001 г. Хотя непосредственные последствия данной трагедии в США, возможно, и не привели к кардинальным изменениям, но послужили переходу к устойчивости к различным угрозам [14].

По мнению S. Mukherjee, современная система безопасности в меньшей степени нацелена на превентивное предотвращение угроз и фокусируется на эффективном реагировании на них и управлении ими [15]. Благодаря всестороннему пониманию тонкостей, присущих корпоративной безопасности, организации получают больше возможностей для упреждающего прогнозирования и эффективного реагирования на широкий спектр экономических, социальных проблем и проблем, связанных с корпоративной безопасностью.

Общие тенденции исследований показали, что большинство авторов рассматривают корпоративную безопасность как комплексную систему, включающую различные аспекты, такие как информационная безопасность, физическая безопасность, кадровая безопасность и т. д. отмечают возрастающее влияние внешних факторов, таких как глобализация, цифровизация и геополитические события, на корпоративную безопасность. Информационные технологии играют все более важную роль в обеспечении корпоративной безопасности. Многие авторы подчеркивают важность человеческого фактора в обеспечении корпоративной безопасности. Корпоративная безопасность должна быть гибкой и адаптироваться к постоянно меняющимся угрозам.

Анализ представленной литературы показал, что исследования в области корпоративной безопасности активно развиваются. Авторы исследуют различные аспекты этой проблемы, предлагают новые подходы и модели. Однако, несмотря на значительный прогресс, многие вопросы остаются открытыми и является основанием для выбора темы данного исследования и обосновывает **целесообразность** ее разработки.

Таким образом, исследование актуально в связи с растущей уязвимостью энергетических компаний перед киберугрозами и необходимостью обеспечения надежной корпоративной безопасности. Основная проблема заключается в создании комплексной системы защиты, учитывающей как внутренние, так и внешние угрозы.

Цель исследования заключается в разработке модели информационной системы управления корпоративной безопасностью для АО «Мосэнергосбыт», которая повысить эффективность предотвращения и реагирования на угрозы, а также обеспечит непрерывность бизнеса.

Задачи исследования:

– идентифицировать ключевые компонентов системы корпоративной безопасности;

– разработать модель информационной системы управления корпоративной безопасностью для АО «Мосэнергосбыт».

Научная новизна исследования в том, что предложена модель цикла управления информационной системой корпоративной безопасности АО «Мосэнергосбыт»», объединяющая технические, организационные и управленческие аспекты. Данное исследование вносит оригинальный вклад в научный дискурс, предлагая новые теоретические концепции и практические инструменты для оценки и повышения уровня корпоративной безопасности.

Теоретическая значимость исследования состоит в обосновании целесообразности совершенствования системы корпоративной безопасности энергетических компаний.

Практическая значимость исследования определяется тем, что результаты могут быть использованы для разработки отраслевых стандартов и улучшения корпоративной безопасности энергетических предприятий России для повышения конкурентоспособности.

Методология исследования основана на системном подходе. В рамках данного подхода используются следующие методы: индукция, дедукция, сравнение и систематизация для изучения существенных характеристик и эволюции базовых понятий. Анализ и синтез также используются для определения ключевых параметров внешних и внутренних угроз корпоративной безопасности энергетического предприятия и характеристики основных противоречий, приводящих к возникновению этих угроз.

В исследовании использовался системный подход к изучению корпоративной безопасности в энергетическом секторе с акцентом на АО «Мосэнергосбыт». Системный подход позволил получить целостное представление о сложных взаимодействиях между различными компонентами системы корпоративной безопасности.

Ключевые методологические элементы включали всесторонний обзор существующей литературы по корпоративной безопасности, информационной безопасности и управлению рисками, особенно в энергетическом секторе. Это обеспечило теоретическую основу для исследования и выявило пробелы в существующих знаниях.

АО «Мосэнергосбыт» было выбрано в качестве тематического исследования, чтобы представить конкретный пример проблем и возможностей, с которыми сталкиваются энергетические компании при повышении своей корпоративной безопасности.

Исследование началось с выявления проблемы обеспечения корпоративной безопасности в энергетическом секторе, сосредоточив внимание на задачах, с которыми сталкивается АО «Мосэнергосбыт». Данные по предприятию АО «Мосэнергосбыт» были собраны из различных источников (документы и отчеты компаний и общедоступные данные об инцидентах, связанных с кибербезопасностью). Результаты анализа данных были использованы для выработки

всестороннего понимания проблем корпоративной безопасности, с которыми сталкивается АО «Мосэнергосбыт», и для проверки правильности предложенной модели. Исследование завершилось обобщением ключевых выводов, обсуждением их последствий для теории и практики и определением областей для будущих исследований.

Основная часть

Необходимость совершенствования корпоративной безопасности на предприятия АО «Мосэнергосбыт» в первую очередь обусловлена двумя фундаментальными факторами. Во-первых, существует необходимость создания безопасной среды для развития бизнеса, которая зависит от присущих коммерческой деятельности рисков и сложного делового климата в России, характеризующегося длительными процессами трансформации и экономической нестабильностью. Во-вторых, растет признание значимости корпораций в современной экономической динамике, их текущего влияния на национальные экономические процессы и их потенциала для будущего развития.

С точки зрения повышения корпоративной безопасности АО «Мосэнергосбыт» определено, что бизнес-операции связаны с риском, поскольку его возникновение определено не только с процессом принятия любых управленческих решений, но и с колебаниями как внешней, так и внутренней среды предприятия. Учитывая, что неблагоприятные последствия реализации риска представляют угрозу, а именно эскалацию корпоративной безопасности, одной из основных задач служб безопасности АО «Мосэнергосбыт» становится обеспечение информационной поддержки руководства с особым акцентом на защиту аспектов деятельности хозяйствующего субъекта с целью снижения угроз и рисков. Рассматривая возникновение риска как проявление повышенного уровня опасности, его снижение путем оценки и информационного обеспечения снизят потенциальные материальные, трудовые и финансовые потери.

По сути, структуру корпоративной системы безопасности АО «Мосэнергосбыт» можно разделить на множество компонентов, которые проявляются в виде горизонтальных функциональных компонентов или подсистем, охватывающих экономическую, технологическую, информационную, правовую, кадровую, транзакционную, логистическую и ресурсную сферы. В рамках каждого отдельного компонента корпоративной структуры существуют функциональные структуры. Компоненты интегрированы в единую систему с помощью корпоративной системы безопасности АО «Мосэнергосбыт», направленной на минимизацию затрат на всю операцию, а не на сосредоточение внимания на отдельных компонентах.

Инструментом, способствующим такой интеграции, является система информационной поддержки корпоративной безопасности. Ключевую роль в данном процессе играет комплексный механизм информационной поддержки. Информационные потоки служат связующими элементами, которые связывают все отдельные компоненты корпоративной безопасности. Одновременно информационная сеть облегчает разработку баз данных, коммуникацию в рамках корпоративной системы безопасности и широкий спектр мер, предназначенных, среди прочего, для процессов принятия оперативных и стратегических решений.

Результаты. Для обспечения эффективности анализа информационной деятельности в рамках корпоративной безопасности крайне важно рассматривать как взаимосвязанную совокупность функционально различных подсистем. Функционирование подсистем регулируется общей информационной системой, которая сама функционирует через входящие в ее состав информационные подсистемы. Хотя такое разделение может показаться несколько произвольным, на практике их сложное взаимодействие и совместная работа необходимы для бесперебойной работы всей системы АО «Мосэнергосбыт». Разработанная модель цикла управления информационной системой корпоративной безопасности АО «Мосэнергосбыт» представлена на рис. 1.

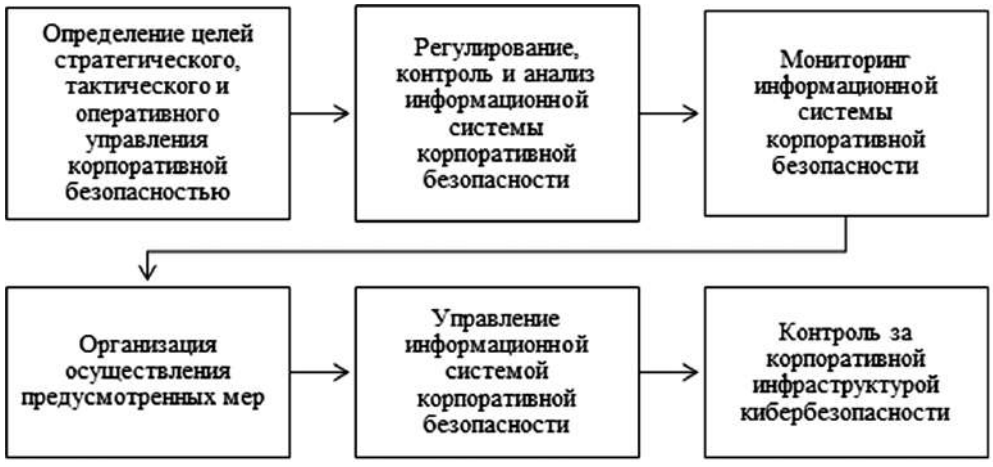

Рис. 1. Схема управления информационной системы корпоративной безопасности АО «Мосэнергосбыт» (разработано автором)

На рис. 1 представлена схема взаимосвязанных компонентов, направленных на постановку стратегических, тактических и оперативных целей управления корпоративной безопасностью, организацию выполнения запланированных мероприятий, регулирование, мониторинг и анализ информационной системы корпоративной безопасности АО «Мосэнергосбыт».

Концепция, основанная на информационной системе, является многообещающей, поскольку она выходит за рамки традиционного подхода, ориентированного на бухгалтерский учет, и охватывает всю целевую корпоративную систему безопасности. Также расширяет базу контроля, поскольку помогает использовать как количественные, так и качественные данные.

Интерпретация концепции управления информационной системой корпоративной безопасности АО «Мосэнергосбыт» в рамках системного подхода, ориентировано на информационную систему. Управление информационной системой корпоративной безопасности — это не просто отдельная функция управления, а скорее инструмент, который будет поддерживать систематический процесс управления корпоративной безопасностью для принятия решений посредством целенаправленного отбора информации. Кроме того, «контроль» дает основания рассматривать управление информационной системой корпоративной безопасности как философскую или концептуальную основу для управления корпоративной безопасностью, которую можно понимать как совокупность точек зрения на определение целей, структурирование и реализацию стратегий стратегического, тактического и оперативного управления в рамках корпоративной безопасности [4].

Разработка корпоративной информационной системы безопасности АО «Мосэнергосбыт» представляет собой сложный и многогранный процесс. Системный подход поможет эффективно управлять всеми процессами за счет использования соответствующих информационных технологий, методологий и форм поддержки общей системы корпоративной безопасности.

Разработка механизмов контроля информационных потоков в рамках системы корпоративной безопасности АО «Мосэнергосбыт» приобретает особое значение в условиях, когда информация и знания воспринимаются как наиболее ценный и дефицитный ресурс, составляющий неотъемлемую часть экономического потенциала всеобъемлющей системы корпоративной безопасности.

Далее представлен общий обзор этапов контроля информационной системы для улучшения корпоративной безопасности АО «Мосэнергосбыт» (см. табл.).

Этапы контроля информационной системы корпоративной безопасности АО «Мосэнергосбыт»

Этап контроля	Описание	Цель
Планирование	Разработка стратегии информационной безопасности, определение целей и задач контроля, выделение ресурсов	Определение направлений деятельности по обеспечению информационной безопасности
Анализ рисков	Идентификация потенциальных угроз, оценка их вероятности и последствий	Определение наиболее уязвимых мест системы и приоритезация мер по их защите
Разработка мер защиты	Создание комплексной системы защиты информации, включающей технические, организационные и административные меры	Минимизация рисков и обеспечение конфиденциальности, целостности и доступности информации
Внедрение мер защиты	Реализация разработанных мер защиты, настройка оборудования и программного обеспечения	Обеспечение функционирования системы защиты в соответствии с установленными требованиями
Мониторинг и анализ	Регулярный контроль состояния системы безопасности, анализ логов и событий, выявление и устранение уязвимостей	Обнаружение и предотвращение инцидентов информационной безопасности
Инцидент-реагирование	Разработка планов реагирования на инциденты, проведение расследований, восстановление системы после инцидентов	Минимизация ущерба от инцидентов и предотвращение их повторения
Обучение персонала	Проведение регулярных тренингов для сотрудников по вопросам информационной безопасности	Повышение уровня осведомленности сотрудников о угрозах информационной безопасности и правилах работы с информационными системами

Примечание: составлено автором.

Для повышения эффективности контроля рекомендуется использовать специализированные программные продукты для управления информационной безопасностью (*SIEM*-системы, системы обнаружения вторжений и т. д.). Также для ускорения разработки и внедрения изменений в систему безопасности необходимо внедрение принципов непрерывной интеграции и непрерывной поставки (*CI*/*CD*).

Регулярная оценка эффективности внедренных мер защиты будет проводиться с использованием различных методик (например, пентестинг). Центральным аспектом планирования и совершенствования корпоративной безопасности АО «Мосэнергосбыт» является достижение баланса между централизацией и децентрализацией в работе ее отдельных компонентов и подсистем. Оптимальное функционирование каждой подсистемы: экономической, технологической, информационной, правовой, кадровой, транзакционной, логистической и ресурсно-ориентированной безопасности — имеет важное значение для общего успеха системы корпоративной безопасности [6].

Однако их изолированная работа, несмотря на их индивидуальные преимущества, может препятствовать достижению оптимальных результатов для всей системы в целом. Поэтому одной из фундаментальных предпосылок успешной работы АО «Мосэнергосбыт» в крупных масштабах является совершенствование информационной системы, способной интегрировать все аспекты корпоративной безопасности и управлять ими как единым целым.

Разработанная модель функционирования механизма управления корпоративной безопасностью АО «Мосэнергосбыт», представленная на рис. 2, призвана гарантировать законность каждого решения, принимаемого органами безопасности. Таким образом, начальный этап предполагает создание информационной базы и разработку нескольких альтернативных вариантов действий механизма управления корпоративной безопасностью АО «Мосэнергосбыт». Разнообразие проявляется также в том факте, что определенные решения принимаются не только сотрудниками внутренней службы безопасности, но и в сотрудничестве с внешними субъектами или исключительно внешними сторонами. Например, борьба с попыткой враждебного поглощения требует согласованных усилий по обеспечению внутренней и внешней безопасности.

В контексте формирования ресурсного обеспечения, включающего финансовые, кадровые, информационные и материальные ресурсы, как имеющиеся в настоящее время, так и находящиеся в резерве или потенциально выделяемые для принятия важнейших решений, влияющих на существование и функционирование предприятия

АО «Мосэнергосбыт», также возникают как альтернативы. Оптимальным выбором является тот, который помогает выполнять поставленные задачи с наименьшими затратами имеющихся ресурсов. Более того, учитывая, что основное внимание в обеспечении механизма управления корпоративной безопасностью АО «Мосэнергосбыт» уделяется отдельным людям, реакция которых на определенные процессы не всегда предсказуема, возрастает важность систематического мониторинга ситуации и обладания способностью регулировать процесс принятия решений.

Рис. 2. Модель функционирования механизма управления корпоративной безопасностью АО «Мосэнергосбыт» (разработано автором)

Заключительный этап предполагает уделение максимального внимания оценке как процесса реализации управленческого решения, так и эффективности действий сотрудников службы безопасности. Эффективность механизма управления корпоративной безопасностью АО «Мосэнергосбыт» зависит от содержания, качества и своевременности предоставляемой информации.

Благодаря эффективной работе корпоративной системы управления безопасностью организация достигает своих целей на определенном уровне. Принято различать четыре уровня организационных целей, и для достижения целей каждого уровня требуется конкретная информация. Информационная структура корпоративной системы безопасности АО «Мосэнергосбыт» будет обладать определенными характеристиками независимо от масштаба проблемы или управляемого процесса, а именно:

1. Реализация стратегических задач корпоративной безопасности.

2. Наличие тактических задач, подчиненных достижению стратегических целей.

3. Правильное согласование информационной поддержки со стратегическими целями.

Оперативный уровень информационно-структурной иерархии предоставляет данные, необходимые для успешного оперативного управления корпоративным аппаратом безопасности. Достижение целей управления среднего уровня возможно благодаря использованию информации, предназначенной для тактического управления корпоративной безопасностью [5]. Стратегическое управление представляет собой вершину иерархической структуры. Поскольку тактические планы формулируются в соответствии со стратегическими стратегиями, детализирующими и уточняющими их основные направления в течение короткого периода. Данные, необходимые для вынесения суждений об их реализации, отличаются от данных оперативного и промежуточного уровней иерархии.

Совершенствование информационной системы и стратегических целей системы корпоративной безопасности АО «Мосэнергосбыт» направлены на обеспечение максимальной адаптации корпоративной информационной инфраструктуры

безопасности к меняющимся условиям микро- и макроэкономической среды с минимальными затратами.

Достижение конкурентных преимуществ за счет эффективной корпоративной системы безопасности имеет решающее значение. Надежная информационная система играет ключевую роль в обеспечении эффективного управления в корпоративной среде АО «Мосэнергосбыт». Процесс основан на сравнении информации о процессе обеспечения корпоративной безопасности с установленными стандартами, нормами или прогнозируемыми данными.

На основе сравнений принимаются обоснованные решения относительно необходимых корректировок системы корпоративной безопасности. Наконец, отслеживается влияние действий руководства АО «Мосэнергосбыт» для обеспечения целостности корпоративной системы информационной безопасности. Система контроллинга служит стратегическим ориентиром, направляющим корпоративную систему безопасности к ее целям. На каждом иерархическом уровне механизм управления информационной системой соответствует конкретным целям. На всех этапах управления одинаково важно отслеживать потоки информации по различным каналам обратной связи, касающиеся промежуточных результатов управления корпоративной безопасностью АО «Мосэнергосбыт» (принятие дополнительных корректирующих мер или использование имеющихся ресурсов).

Заключение

Совершенствование информационной системы является важнейшим компонентом системы управления корпоративной безопасностью АО «Мосэнергосбыт». Его разработка и функционирование зависят от специфики финансово-экономических операций, а также от процесса обеспечения корпоративной безопасности.

Предложенная модель механизма отражает сложность системы управления корпоративной безопасностью АО «Мосэнергосбыт». Создание такого механизма должно расширить перечень существующих инструментов, чтобы дать возможность субъектам безопасности достигать своих целей. Разработанные методические рекомендации направлены на повышение динамической адаптивности корпоративной безопасности, способности быстро реагировать на возрастающее негативное воздействие внутренних и внешних угроз, а также ориентацию на поиск ранее неиспользованных внутренних резервов и внешних возможностей предприятия.

Результаты исследования могут быть использованы для повышения уровня безопасности энергетических компаний и обеспечения непрерывности их деятельности. Следовательно, существует настоятельная необходимость в дальнейшем изучении стратегических аспектов управления корпоративной безопасностью.

СПИСОК ИСТОЧНИКОВ

1. Лю Х., Рахимжанова Г. Стратегические подходы к корпоративному управлению: перспективы для обеспечения экономической безопасности // Izdenister Natigeler. 2024. № 2(102). С. 572—579. (На англ. яз.) DOI: 10.37884/2-2024/56.

2. Reka S. Examining the Strategic Embeddedness of Corporate Security // The Eurasia Proceedings of Educational and Social Sciences. 2024. Vol. 32. Pp. 151—157. DOI: 10.55549/epess.1412834.

3. The development of corporate security in the context of countering threats to doing business / T. Shyra, K. Salyga, V. Derii et al. // Business: Theory and Practice. 2021. Vol. 22. Iss. 1. Pp. 211—221. DOI: 10.3846/btp.2021.13396.

4. Wu J. A Security Assessment Strategy for Corporate Financial Systems Based on Data Mining Techniques // Applied Mathematics and Nonlinear Sciences. 2024. Vol. 9. Iss. 1. Pp. 1—16. DOI: 10.2478/amns-2024-1880.

5. Истратов Б. И. Корпоративная безопасность как аспект устойчивого развития бизнеса // Экономика устойчивого развития. 2022. № 1. С. 40—44. DOI: 10.37124/20799136_2022_1_49_40.

6. Леванова Л. Н., Вавилина А. В. Корпоративная безопасность: стейкхолдерский подход // Вестник МИРБИС. 2022. № 3(31). С. 128—142. DOI: 10.25634/MIRBIS.2022.3.14.

7. Никитина И. А., Хмелевской К. В., Назаров П. В. Вопросы оценки угроз кадровой безопасности организации в современных условиях // Инновации и инвестиции. 2023. № 11. С. 150—153.

8. Соколова Е. О., Коренчук Я. А. Роль корпоративной культуры в обеспечении кадровой безопасности организации // Журнал социологических исследований. 2024. Т. 9. № 1. С. 51—57.

9. Фролов А. В., Дымченко Ю. В. Корпоративная безопасность и обеспечение защиты данных от утечки в условиях удаленной работы // Промышленные АСУ и контроллеры. 2023. № 9. С. 47—49.

10. Якушкина А. А., Юмангулов А. Ф. Кадровая безопасность как одна из составляющих экономической безопасности // XI Международный молодежный симпозиум по управлению, экономике и финансам : сб. науч. тр. Казань : Изд-во Каз. (Приволж.) федер. ун-та, 2022. С. 758—761.

11. Baschung D., Gillard S., Metzger J. C., Keupp M. M. Individual Career Versus Corporate Security: A Simulation of CSO Investment Choices // Cyberdefense. The Next Generation / ed. M. M. Keupp. Cham : Springer, 2023. Pp. 163—181. (International Series in Operations Research & Management Science; vol. 342). DOI: 10.1007/978-3-031-30191-9_11.

12. Volosnikova N. Research of sustainability of the general corporate security system // Bulletin of the National Technical University Kharkiv Polytechnic Institute (economic sciences). 2021. № 1. Pp. 41—47. DOI: 10.20998/2519-4461.2021.1.41.

13. Yıldız E. P., Simsekler O. Corporate Cyber Security In Turkey Investigation Of Legal And Corporate Infrastructure: A Meta-Synthesis Study // Global Journal of Computer Sciences Theory and Research. 2023. Vol. 13. Iss. 1. Pp. 46—58. DOI: 10.18844/gjcs.v13i1.8858.

14. Milica D. The Corporate Security at a Global Scale // Global Journal of Social Sciences Studies. 2022. Vol. 8. No. 2. Pp. 56—61. DOI: 10.55284/gjss.v8i2.730.

15. Mukherjee S. Overview of the Importance of Corporate Security in business // International Journal of Innovative Research in Science, Engineering and Technology. 2019. Vol. 8. Iss. 4. Pp. 3651—3657.

REFERENCES

1. Liu H., Rahimzhanova G. Strategic approaches to corporate governance: prospects for ensuring economic security. *Izdenister natigeler*. 2024;2(102):572—579. DOI: 10.37884/2-2024/56.

2. Reka S. Examining the Strategic Embeddedness of Corporate Security. *The Eurasia Proceedings of Educational and Social Sciences*. 2024;32:151—157. DOI: 10.55549/epess.1412834.

3. Shyra T., Salyga K., Derii V. et al. The development of corporate security in the context of countering threats to doing business. *Business: Theory and Practice*. 2021;22(1):211—221. DOI: 10.3846/btp.2021.13396.

4. Wu J. A Security Assessment Strategy for Corporate Financial Systems Based on Data Mining Techniques. *Applied Mathematics and Nonlinear Sciences*. 2024;9(1):1—16. DOI: 10.2478/amns-2024-1880.

5. Istratov B. I. Corporate security as an aspect of sustainable business development. *Ekonomika ustoichivogo razvitiya = Economics of stable development*. 2022;1:40—44. (In Russ.) DOI: 10.37124/20799136_2022_1_49_40.

6. Levanova L. N., Vavilina A. V. Corporate security: stakeholder approach. *Vestnik MIRBIS*. 2022;3(31):128—142. (In Russ.) DOI: 10.25634/MIRBIS.2022.3.14.

7. Nikitina I. A., Khmelevskoi K. V., Nazarov P. V. Issues of assessing threats to enterprise personnel security in modern conditions. *Innovatsii i investitsii*. 2023;11:150—153. (In Russ.)

8. Sokolova E., Korenchuk Ya. The role of corporate culture in ensuring the personnel security of the organization. *Zhurnal sotsiologicheskikh issledovanii*. 2024;9(1):51—57. (In Russ.)

9. Frolov A. V., Dymchenko Yu. V. Corporate Security and Data Leakage Protection in Remote Work Conditions. *Promyshlennye ASU i kontrollery = Industrial Automatic Control Systems and Controllers*. 2023;9:47—49. (In Russ.)

10. Yakushkina A. A., Yumangulov A. F. Personnel security as one of the components of economic security. XI International Youth Symposium on Management, Economics and Finance. Collection of scientific papers. Kazan, Kazan (Volga) Federal University publ., 2022:758—761. (In Russ.)

11. Baschung D., Gillard S., Metzger J. C., Keupp M. M. Individual Career Versus Corporate Security: A Simulation of CSO Investment Choices. *Cyberdefense. The Next Generation*. International Series in Operations Research & Management Science; vol. 342. M. M. Keupp (ed.). Cham, Springer, 2023. Pp. 163—181. DOI: 10.1007/978-3-031-30191-9_11.

12. Volosnikova N. Research of sustainability of the general corporate security system. *Bulletin of the National Technical University Kharkiv Polytechnic Institute (economic sciences)*. 2021;1:41—47. DOI: 10.20998/2519-4461.2021.1.41.

13. Yıldız E. P., Simsekler O. Corporate Cyber Security In Turkey Investigation Of Legal And Corporate Infrastructure: A Meta-Synthesis Study. *Global Journal of Computer Sciences Theory and Research*. 2023;13(1):46—58. DOI: 10.18844/gjcs.v13i1.8858.

14. Milica D. The Corporate Security at a Global Scale. *Global Journal of Social Sciences Studies*. 2022;8(2):56—61. DOI: 10.55284/gjss.v8i2.730.

15. Mukherjee S. Overview of the Importance of Corporate Security in Business. *International Journal of Innovative Research in Science, Engineering and Technology*. 2019;8(4):3651—3657.

Статья поступила в редакцию 30.09.2024; одобрена после рецензирования 17.10.2024; принята к публикации 21.10.2024.
The article was submitted 30.09.2024; approved after reviewing 17.10.2024; accepted for publication 21.10.2024.