About the author:
LEPEHANOVA Darya Sergeevna – Student, Tver State Technical University, Tver. E-mail: darya.lepehanova@mail.ru
Research manager – Skvortsova Galina Gennadyevna, Candidate of Economic Sciences, Associate Professor of the Department of Economics and Production Management, Tver State Technical University, Tver. E-mail: gala-skvortsova@yandex.ru

УДК 331.108

ПРОБЛЕМЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Ю.Д. Нестерова

© Нестерова Ю.Д., 2025

Аннотация. *В статье рассмотрена актуальная проблема сохранения информационной безопасности хозяйствующих субъектов. Отмечено, что главные угрозы информационной безопасности связаны с персоналом организации и устранить их могут только грамотные ИТ-специалисты.*

Ключевые слова: *информационная безопасность, персонал организации, кадровое обеспечение*.

Информация – один из самых ценных ресурсов, которые могут использовать компании для достижения своих целей и повышения конкурентоспособности на рынке. В условиях развития информационного общества и постоянного роста объемов обрабатываемых данных вопрос информационной безопасности становится не просто актуальным, а критически важным для любого хозяйствующего субъекта.

Под информационной безопасностью подразумевается комплекс мер, направленных на защиту информации от различных угроз, таких как несанкционированный доступ, утечка, искажение, а также полное уничтожение данных.

Информационная безопасность охватывает множество аспектов, связанных с защитой информации, которая находится в распоряжении организации. При этом ключевыми элементами информационной безопасности являются конфиденциальность, целостность и доступность сведений. Конфиденциальность – это защита данных от несанкционированного доступа, целостность – сохранение точности и полноты

информации, а доступность – возможность получения данных в нужный момент.

Основная задача руководства любой компании заключается в том, чтобы обеспечить доступность и целостность информации для своих сотрудников и при этом ее конфиденциальность, т.е. защиту от конкурентов и мошенников.

В современных условиях информационная безопасность имеет огромное значение для функционирования любого бизнеса. Это связано с несколькими факторами.

Во-первых, на сегодняшний день успешные компании активно используют информацию в различных процессах – от стратегического планирования и разработки бизнес-планов до оперативного управления и контроля за выполнением задач. Утечка, искажение или уничтожение данных могут привести к серьезным последствиям для бизнеса, включая репутационные и финансовые потери, уход клиентов.

Во-вторых, с ростом цифровизации экономики и внедрением современных информационных технологий в повседневную практику организаций повышаются риски, связанные с безопасностью данных. Компании все чаще сталкиваются с угрозами, исходящими от киберпреступников, которые могут попытаться получить доступ к конфиденциальной информации или же навредить системам, на которых эта информация хранится. Таким образом, необходимость принятия эффективных мер по обеспечению информационной безопасности становится особенно актуальной.

Известно, что уязвимость любой системы оценивается по наиболее слабому ее звену. Во многих исследованиях отмечается, что при обеспечении информационной безопасности таковым является именно человек.

Внешние и внутренние утечки информации, а также полная утрата данных представляют серьезную угрозу для любой организации, но все они так или иначе связаны с человеком.

Внешние утечки обычно вызваны несанкционированными действиями внешних злоумышленников, которыми могут быть хакеры и киберпреступники. Они проводят кибератаки, взламывают системы с целью получения доступа к конфиденциальным данным или создания сбоев в работе таких систем.

Злоумышленники используют не столько недостатки оборудования и программного обеспечения (постоянно меняющегося и совершенствующегося), сколько отсутствие должной дисциплины в коллективе и контроля на рабочих местах пользователей.

Внутренние утечки могут возникать из-за ошибок или намеренных действий персонала организации, в результате которых конфиденциальная информация попадает к лицам, не имеющим к ней доступа (конкурентам).

В этом случае субъектом угроз информационной безопасности могут быть не только работники, состоящие в трудовых отношениях с работодателем. Обоснованным представляется включение в их состав соискателей вакантных должностей. В этой роли могут выступать представители конкурирующих организаций, криминальных структур, хедхантеры [см. библиографический список].

Кроме того, большую угрозу представляют и бывшие работники организации. Особенно те, которые покинули рабочее место не по своей инициативе.

Решение перечисленных проблем требует комплексного и многостороннего подхода. Однако в этой связи исключительное значение приобретает кадровое обеспечение информационной безопасности. Необходимы квалифицированные ИТ-специалисты в области защиты информации и обеспечения информационной безопасности предприятия. За последние десять лет количество таких специалистов постепенно растет. По итогам 2024 г. число специалистов по информационной безопасности в России достигло 992 тыс. человек. Это на 16 % больше по сравнению с 2023 г., о чем 19 марта 2025 г. сообщил министр цифрового развития Российской Федерации Максут Шадаев. Тем не менее в отрасли сохраняется значительный дефицит кадров. Экономике России сегодня требуется еще около 100 тыс. разработчиков программного обеспечения и 40 тыс. специалистов по базам данных и сетям. Это известно из доклада министра труда и социальной защиты Российской Федерации Антона Котякова.

Именно ИТ-специалисты совместно с руководителями предприятий должны разработать комплекс мер по обеспечению информационной безопасности предприятия.

Во-первых, необходимо усилить физическую безопасность, включая охрану здания, видеонаблюдение, внедрение пропускного режима, создание службы безопасности и другие меры предосторожности, чтобы предотвратить несанкционированный доступ к оборудованию и информационным системам.

Во-вторых, требуется разработать и внедрить политику информационной безопасности, согласно которой будут определены зоны ответственности работников, инструктажи для персонала, установлен запрет на пересылку служебной информации на личную электронную почту, порядок обращения с секретными данными, определены средства получения доступа сотрудников и других лиц к данным и системам, а также установлены процедуры ответа на инциденты безопасности и проведены проверки безопасности.

В-третьих, важно обучить персонал основам информационной безопасности и внести это в корпоративную культуру. Сотрудники должны быть осведомлены о возможных угрозах и способах их предотвращения, а

также о том, как правильно использовать системы и следовать политике безопасности. Для этого следует выпускать информационный бюллетень раз в несколько месяцев с информацией о новых угрозах и мерах защиты, внедренных компанией. Без создания такой культуры все технические меры защиты не смогут справиться с ошибками, допускаемыми сотрудниками, а сами работники не будут в полной мере осознавать важность проблемы.

Чтобы исключить появление внутри предприятия потенциальных злоумышленников, нужно тщательно проверять кандидатов при отборе персонала, подробно изучать их человеческие качества, а также использовать современные технические, цифровые и электронные средства противодействия.

Таким образом, решение проблем кадрового обеспечения информационной безопасности остается одной из ключевых задач для организаций в условиях быстро меняющихся технологий и растущих угроз.

Библиографический список

Грачев С.А., Гундорова М.А. Обеспечение экономической безопасности предприятия: учебное пособие. Владимир: ВлГУ, 2022. 420 с.

PROBLEMS OF STAFFING OF INFORMATION SECURITY OF THE ORGANIZATION

Yu.D. Nesterova

Abstract. *The article considers the actual problem of preserving the information security of business entities. It is noted that the main threats to information security are related to the personnel of the organization and only competent IT specialists can eliminate them.*

Keywords: *information security, organization personnel, human resources.*

Об авторе:

НЕСТЕРОВА Юлия Дмитриевна – студентка, ФГБОУ ВО «Тверской государственный университет», Тверь. E-mail: ylonesh@mail.ru

Научный руководитель – Нестерова Ксения Игоревна, кандидат экономических наук, заведующая кафедрой управления персоналом, ФГБОУ ВО «Тверской государственный университет», Тверь. E-mail: nksusa@rambler.ru

About the author:
NESTEROVA Yulia Dmitrievna – Student, Tver State University, Tver. E-mail: ylonesh@mail.ru
Research manager – Nesterova Ksenia Igorevna, Candidate of Economic Sciences, Head of the Department of Human Resources Management, Tver State Technical University, Tver. E-mail: nksusa@rambler.ru

УДК 338.1:341.655(470+571)

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ РОССИЙСКИХ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ САНКЦИЙ

М.В. Осадчая

© Осадчая М.В., 2025

Аннотация. *В статье исследованы стратегии экономической безопасности российских промышленных предприятий в условиях санкционного давления. Проанализированы основные категории санкций и их влияние на российскую промышленность. Рассмотрены ключевые стратегии минимизации негативных последствий, в том числе импортозамещение, привлечение иностранного капитала, переориентация на новые рынки и диверсификация логистических цепочек. На примере автомобильной промышленности показаны успехи и ограничения политики импортозамещения, а также имеющаяся зависимость от иностранных технологий и компонентов. Особое внимание уделено проблеме отставания в сфере научно-исследовательских и опытно-конструкторских работ и необходимости ускоренного развития отечественных технологий для обеспечения долгосрочной экономической безопасности.*

Ключевые слова: *экономическая безопасность, промышленные предприятия, санкции, импортозамещение, стратегии адаптации, автомобильная промышленность, технологическая зависимость.*

Первые политические и экономические санкции в отношении России со стороны США и стран ЕС были введены в 2012 г. В последующие годы количество антироссийских ограничений неизменно увеличивалось, а поводы для этого постоянно менялись.

С начала проведения специальной военной операции (февраль 2022 г.) уже более 60 стран, включая США, Канаду, государства Европейского союза, Великобританию, Новую Зеландию и Японию, ввели и поэтапно