$$\Delta ГВ(У_д) = \Delta У_{д1} \cdot Д \cdot П_0 \cdot ЧВ_0 = (-0,03) \cdot 214 \cdot 7,8 \cdot 66,89 = -3424,03 \text{ руб.};$$

– количества отработанных дней одним рабочим за год:

$$\Delta ГВ(Д) = \Delta У_{д1} \cdot \Delta Д \cdot П_0 \cdot ЧВ_0 = 0,82 \cdot (-3)7,98 \cdot 66,89 = -1319,43 \text{ руб.};$$

– продолжительности рабочей смены:

$$\Delta ГВ(П) = У_{д1} \cdot Д1 \cdot \Delta П \cdot ЧВ_0 = 0,82 \cdot 211 \cdot 0,02 \cdot 66,89 = 232,58 \text{ руб.};$$

– среднечасовой выработки рабочего:

$$\Delta ГВ(ЧВ) = У_{д1} \cdot Д_1 \cdot П_1 \cdot \Delta ЧВ = 0,82 \cdot 211 \cdot 8 \cdot 0,24 = 333,82 \text{ руб.}$$

Исходя из полученных расчетов понятно, что сокращение удельного веса рабочих на 0,03 повлекло за собой сокращение среднегодовой выработки на сумму 3424,03 руб., а также количество отработанных дней одним рабочим за год сократилось на 3 дня, что также привело к сокращению среднегодовой выработки на сумму 1319,43 руб.

С учетом показателей, сокращающих значение производительности труда, можно предложить следующие пути повышения данного показателя: для увеличения численности рабочих необходимо создать комфортные условия на рабочих местах, а также улучшить систему мотивирования; для сокращения количества неявок на работу по причине болезни необходимо внедрить систему стимулирования, направленную на оздоровление работников (путевки в санаторий, медицинское страхование и т. п.).

Таким образом, для увеличения производительности труда нужно выполнить следующие меры: обеспечить полноценную загрузку производственных мощностей, усовершенствовать логистику предприятия, автоматизировать производственные процессы, совершенствовать управленческие, организационные структуры, повысить квалификацию сотрудников на курсах, обеспечить соблюдение трудовой дисциплины в коллективе. Это поможет достигнуть следующих результатов: увеличить количество произведенной продукции без ущерба для качества, повысить качество произведенной продукции, снизить трудовые затраты на производство единицы товара и сократить общую долю трудозатрат в себестоимости продукции.

Литература

1. Алексеева, А. И. Комплексный экономический анализ хозяйственной деятельности / А. И. Алексеева. – М. : Финансы и статистика, 2020. – 526 с.
2. ОАО «Речицкий метизный завод». – Режим доступа: https://rmz.by/about-the-company/financial-statements/. – Дата доступа: 01.02.2024.
3. Савицкая, Г. В. Анализ хозяйственной деятельности / Г. В. Савицкая. – Минск : РИПО, 2024. – 374 с.

ПРОБЛЕМА ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

А. А. Григорян

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Г. В. Митрофанова

Рассмотрены основные составляющие информационной безопасности, такие как целостность, конфиденциальность и доступность информации. Описаны различные мероприятия и

виды контроля, необходимые для обеспечения полноценной и надежной защиты данных. Подчеркнута необходимость комплексного и системного подхода к обеспечению информационной безопасности. Показано применение различных видов контроля, таких как административный, логический и физический.

Ключевые слова: информационная безопасность, целостность, конфиденциальность, доступность, комплексный подход, системный подход, административный контроль, логический контроль, физический контроль.

Проблема передачи и защиты информации в современной организации в Республике Беларусь (РБ) является актуальной и требует особого внимания. В цифровую эпоху, когда информация стала одним из ключевых активов предприятий, обеспечение ее безопасности становится важным аспектом успешной деятельности организации. Основные составляющие информационной безопасности – это целостность информации, ее конфиденциальность и доступность. Под целостностью понимается свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Конфиденциальность информации – это свойство информации быть известной и доступной только правомочным субъектам (программам, процессам, пользователям). Доступность – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных субъектов к интересующей их информации [1].

Известно, что процесс массового внедрения компьютерной техники и информационных технологий наряду с прогрессивным началом неизбежно создает и дополнительные проблемы. Они связаны с реальными угрозами безопасности предприятий, с потерей стратегически важной информации, а вместе с этим и утратой управляемости компании. В целях сокращения побочных явлений повсеместного использования новых информационных технологий руководство организаций определяет стратегию своей деятельности в информационной сфере. Стержнем такой стратегии должна быть информационная безопасность, определяемая как состояние защищенности интересов предприятий или организации в информационной сфере. Все направления деятельности предприятия, в которых прямо или косвенно используются информационные технологии, фокусируются в рамках обеспечения информационной безопасности [2].

Защита информации включает в себя: комплекс организационных мероприятий, комплекс технических мероприятий.

Рассмотрим примеры мер, которые организация может предпринять для улучшения безопасности предприятия:

• Внедрение двухфакторной аутентификации.

Организация будет требовать от сотрудников использовать два различных метода аутентификации для доступа к системам и приложениям. Например, помимо пароля может быть использовано одноразовое смс-сообщение или аутентификатор на основе временных кодов. Это значительно повышает безопасность, так как для взлома учетных данных требуется не только знание пароля, но и доступ к дополнительному фактору.

• Создание комплексных паролей.

Организация может требовать от сотрудников использовать сложные и уникальные пароли для своих учетных записей. Рекомендуется использовать комбинацию букв, цифр и специальных символов, а также избегать очевидных или легко угадываемых паролей.

• Установка систем мониторинга и обнаружения инцидентов.

Организация внедрит специализированные системы мониторинга и обнаружения

инцидентов, которые будут контролировать сетевую активность, регистрировать аномальное поведение и предупреждать об возможных угрозах безопасности. Это позволит оперативно реагировать на инциденты и предотвращать потенциальные атаки.

• Резервное копирование данных.

Организация должна регулярно создавать резервные копии всех важных данных. Резервное копирование помогает восстановить информацию в случае ее потери или повреждения в результате атаки или сбоя системы. Резервные копии должны храниться на отдельных и защищенных устройствах или в облачных хранилищах.

Обеспечить полноценную и надежную информационную безопасность предприятия можно только при условии применения комплексного и системного подхода. Существует несколько видов контроля информационной безопасности, внедрение которых позволяет компании снижать риски в этой сфере и поддерживать их на приемлемом уровне. Здесь различают административный контроль, логический контроль и физический контроль.

Административный контроль информационной безопасности – это система, состоящая из комплекса установленных стандартов, принципов и процедур. Этот вид контроля определяет границы для осуществления бизнес-процессов и управления персоналом. Он включает законодательные и нормативные акты, принятую на предприятии политику корпоративной безопасности, систему найма сотрудников, дисциплинарные и другие меры. Административный контроль информационной безопасности нужен для обеспечения защиты информации от несанкционированного доступа, использования, изменения, уничтожения или раскрытия.

Логический контроль предусматривает использование средств управления (средств технического контроля), которые защищают информационные системы от нежелательного доступа.

Физический контроль сосредоточен на среде рабочих мест и средствах вычисления. В том числе он предусматривает обеспечение эффективного функционирования инженерных систем зданий предприятия, работа которых может повлиять на хранение и передачу информации. К таким системам относятся отопление и кондиционирование, противопожарные системы. Физический контроль информационной безопасности необходим для защиты физических ресурсов, таких как серверы, коммуникационное оборудование, хранилища данных и т. д. [3].

Таким образом, обеспечение информационной безопасности является неотъемлемым процессом функционирования предприятий, основными составляющими которого являются целостность информации, ее конфиденциальность и доступность. Для обеспечения полноценной и надежной информационной безопасности необходим комплексный и системный подход, включающий в себя организационные и технические мероприятия, а также различные виды контроля информационной безопасности, такие как административный, логический и физический контроль.

Литература

1. Режим доступа: https://rtmtech.ru/articles/problemy-zashhity-informatsii-na-predpriyatii/. – Дата доступа: 28.10.2023.
2. Режим доступа: https://prog.bobrodobro.ru/20191. – Дата доступа: 28.10.2023.
3. Режим доступа: https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/. – Дата доступа: 28.10.2023.