экономики: материалы IX Междунар. науч.-практ. конф. (г. Омск, 03 июня 2021 г.). – Омск: Изд-во Омский гос. ун-т путей сообщения, 2021. – Ч. 2. – С. 174-183.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ КАК ЭЛЕМЕНТ КОРПОРАТИВНОЙ КУЛЬТУРЫ ОРГАНИЗАЦИИ

Хололович Д.В., Носко Н.В.
УО «БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ», г. Брест

В век информационных технологий и инноваций большинство организаций сталкиваются с угрозами безопасности информационных активов. В защите от внутренних и внешних угроз нуждаются не только физические, но и информационные активы. Угроза информационной безопасности организации – это ряд факторов и условий, которые создают риски, в следствии нарушения безопасности, которые вызывают или способны принести организации вред или ущерб [1]. Таким образом, последствия таких угроз могут вызвать как экономические потери, так и нанести ущерб репутации компании в целом.

Угрозы, которым подвергаются предприятия, включают как преднамеренные, так и непреднамеренные угрозы.

К преднамеренным угрозам относятся разговоры с неуполномоченными лицами на конфиденциальные темы, обмен информацией ограниченного доступа, передача носителей информации неуполномоченным лицам и публичные заявления.

К непреднамеренным угрозам относятся: потеря носителя, содержащего информацию ограниченного доступа, копирование информации на незарегистрированный носитель, разговор об информации ограниченного доступа вне специально отведенных помещениях, где посторонние лица могут преднамеренно подслушивать, работа с информацией ограниченного доступа на незащищенном оборудовании или автоматизированных системах, возможна работа с информацией ограниченного доступа (конфиденциальные сообщения) при выключенной системе, а также невыполнении организационных мероприятий по защите информации; передачу информации ограниченного доступа по незащищённым каналам связи [2].

Такие угрозы могут быть вызваны халатностью сотрудников компании, игнорированием своих обязанностей или, прежде всего, действиями отдельных лиц, действующих в собственных интересах.

Сегодня стало возможным предотвратить утечку информации из компаний. Для этого необходимо либо создать сильную корпоративную культуру, либо изменить уже сложившуюся организационную культуру. Были предложены различные трактовки этого явления, но суть достаточно унифицирована. Это система ценностей, принципов, привычек и правил поведения, которые связывают, разделяют и реализуют все сотрудники.

Такая система позволяет каждому в организации двигаться в одном направлении, чувствовать себя и быть признанным частью целого. Несомненно, сильная корпоративная культура делает организацию более эффективной.

Формирование корпоративной культуры является необходимым этапом в развитии любой организации, независимо от сферы ее деятельности. Компании могут работать с информацией, включая коммерческую тайну, персональные данные и государственную тайну. Сотрудники должны быть внимательны и осторожны при работе с такой информацией. Все сотрудники несут ответственность за безопасный доступ к информации, полученной в соответствии с их должностными обязанностями, подвергаются регулярной проверке знаний нормативных требований при работе с конфиденциальной информацией и должны быть морально устойчивы по отношению к общественности (коррупция, злоупотребление властью).

Формирование культуры информационной безопасности включает в себя цикл предоставления информации, обучения, мониторинга, обнаружения нарушений, проверки, расследования и дисциплинарных мер. Предоставление информации предполагает разъяснение сотрудникам вопросов информационной безопасности и ознакомление их с соответствующими внутренними и внешними документами.

Обучение персонала включает в себя изучение внутреннего материала по информационной безопасности и тестирование на основе изученного материала. Надзор предполагает регулирование поведения сотрудников, работающих с конфиденциальной информацией на рабочем месте.

Для выявления нарушений необходимы регулярные аудиты, инсценировка инцидентов информационной безопасности для проверки реакции и поведения сотрудников организации. При обнаружении угрозы необходимо провести расследование для выявления виновного и принять дисциплинарные меры.

Это означает, что информационная безопасность должна быть интегрирована в общую систему управления организацией и практически стать ее частью. Решить эту проблему можно путем: во-первых, внесением положений в области информационной безопасности в общую политику,

цели и концепции организации; во-вторых, необходимостью учитывать риски при планировании, формировании и исполнении бюджета; в-третьих, внедрением принципа неотвратимости наказания.

В то же время необходимо подчеркнуть, что в организации необходимы дополнительные (формальные или неформальные) правила стимулирования, чтобы сотрудники следовали определенной модели поведения, с дополнительными выгодами для работника, так как информация очень важна для успешного развития бизнеса, а значит, нуждается в защите. Особенно актуально это стало в бизнес-среде, где информационные технологии вышли на первый план. В связи с тем, что мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Литература

1. ГОСТ Р 53114-2008 Защита информации обеспечение информационной безопасности в организации. Основные термины и определения.
2. Хорев, А.В. Защита информации: учеб. пособие для студентов вузов. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2019. – 286 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕНЕДЖМЕНТЕ

Хомич В.В., Мочалова Я.В.*
ФГАОУ В «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ», г. Белгород

Характерной особенностью нынешнего периода является переход к информационному обществу, в котором роль знаний, информации и информационных технологий в жизни общества увеличивается. Они приобретают первостепенное значение. В данный период времени эффективное решение задач управления и принятия решений в сложных экономических ситуациях неотрывно связано с информационными технологиями. Сфера управления информацией – это совокупность всех решений, необходимых для управления на всех этапах жизненного цикла предприятия, включая все действия и операции, относящиеся как к информации во всех её формах и состояниях, так и к предприятию в целом.

Менеджмент – это совокупность инновационных технологий, методов, принципов, средств и конфигураций управления, направленных на увеличение производительности разнообразных предприятий.