

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Войтешёнок В. А., Голубев Р. С., студенты
Научный руководитель – Карсеко А. Е., ст. преподаватель
каф. «Экономика и право»
Белорусский национальный технический университет
г. Минск, Республика Беларусь

Как однажды сказал Бенджамин Дизраэли, «как правило, наибольшего успеха добивается тот, кто располагает лучшей информацией» [1]. Вышеупомянутая цитата в полной мере описывает важность информации, а то, что является важным, нуждается в защите. Данную задачу выполняет менеджмент информационной безопасности.

На законодательном уровне понятие «информационная безопасность» закреплено в Концепции информационной безопасности Республики Беларусь, подписанной Президентом Республики Беларусь 18 марта 2019 года. Под ней понимается «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере» [2].

На государственном уровне в первую очередь решаются вопросы обеспечения информационной безопасности в банковской, финансовой и оборонной сферах, системе государственного управления. Вопросы обеспечения информационной безопасности отдельных хозяйствующих субъектов во многом зависят от эффективности корпоративного управления ею.

Поскольку обеспечение информационной безопасности является трудноуправляемым процессом, важность качества менеджмента в данной области возрастает в разы. Ключевыми проблемами в данной области являются слишком большой поток информации, постоянное совершенствование способов незаконного завладения, а также неавторизованного изменения, создания или уничтожения информации, сложность создания системы разграничения полномочий, высокая зависимость от зарубежного программного обеспечения и пр. Решение этих проблем невозможно без создания на предприятиях специализированных структурных подразделений,

отвечающих за эффективное управление потоками информации и обеспечение информационной безопасности, что требует организации подготовки соответствующих специалистов в высших учебных заведениях.

Специалисты в области менеджмента информационной безопасности должны быть знакомы с требованиями международного (ISO 27001) и национального (приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62) законодательства по проектированию систем информационной безопасности, должны уметь разрабатывать политику компании в сфере информационной безопасности и иную документацию, регламентирующую процессы её обеспечения, в том числе простые и понятные регламенты и правила обеспечения информационной безопасности для всех сотрудников компании, проводить проверку соблюдения сотрудниками данных правил, должны уметь разрабатывать, тестировать, внедрять в эксплуатацию системы защиты информации, эффективно управлять ими, оперативно выявлять и расследовать инциденты, связанные с созданием угрозы информационной безопасности компании, анализировать их причины, изучать национальный и мировой опыт борьбы с киберпреступностью и мн. др.

Список литературы

1. Веснин, В. Р. Менеджмент / В. Р. Веснин. – 4-е изд., перераб. и доп. – Москва : Проспект, 2015. – 613 с.
2. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]. – Режим доступа: <https://www.sb.by/articles/kontseptsiya-informatsionnoy-bezopasnosti-respubliki-belarus.html>. – Дата доступа: 13.09.2019.
3. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. №62 «О некоторых вопросах технической и криптографической защиты информации» [Электронный ресурс]. – Режим доступа: <https://oac.gov.by/public/content/files/files/law/prikaz-oac/2013%20-%2062.pdf>. – Дата доступа: 13.09.2019.