УДК 004

Андрей Чудин
(Российская Федерация)
Научный руководитель А.И. Попов, к.п.н., доцент
Тамбовский государственный технический университет

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

В современном мире информационные технологии играют все более важную роль в различных сферах деятельности, включая хозяйственную деятельность. Однако существование информационных технологий также повышает риск различных информационных угроз, что может привести к серьезным последствиям, вплоть до финансовых потерь и потери деловой репутации.

Проблема информационной безопасности хозяйствующих субъектов очень актуальна и требует внимания со стороны бизнеса, государственных органов и общества в целом. Одной из основных причин возникновения проблемы является развитие информационных технологий и все большая потребность в их использовании в деловой деятельности. Но при этом, не все компании уделяют достаточное внимание вопросам информационной безопасности, что ставит их в уязвимое положение перед потенциальными угрозами.

Среди основных угроз информационной безопасности хозяйствующих субъектов можно выделить следующие: киберпреступность, внутренние угрозы, социальная инженерия, мобильная безопасность, недостаточные меры безопасности.

Чтобы минимизировать риски информационной безопасности, хозяйствующие субъекты должны принять ряд мер:

1. Обучение персонала: сотрудники должны быть ознакомлены с основными правилами информационной безопасности и знать, как обеспечить безопасность своей работы. Обучение должно проводиться регулярно и включать в себя обновление информации по новым видам угроз.
2. Создание политики безопасности: компании должны разработать и внедрить политику безопасности, которая будет ясно определять требования к использованию информационных технологий и меры по обеспечению безопасности.

Существует несколько причин, по которым нужно защищать хозяйствующие субъекты в области технологий:

1. Экономические интересы: Хозяйствующие субъекты в области технологий вкладывают большие средства и усилия для разработки новых продуктов и услуг. Если их интеллектуальная собственность будет незащищена, другие компании или лица смогут несправедливо воспользоваться их результатами и получить неоправданную выгоду.

2. Инновации и развитие: Защита хозяйствующих субъектов в области технологий способствует стимулированию инноваций. Если компании знают, что их интеллектуальная собственность будет защищена, они будут более склонны вкладывать средства в исследования и разработки новых технологий.

3. Развитие конкуренции: Защита хозяйствующих субъектов в области технологий помогает поддерживать здоровую конкуренцию в отрасли. Если компании имеют возможность зарегистрировать и защитить свои изобретения или технологии, это дает им преимущество на рынке и способствует разнообразию продуктов и услуг.

4. Защита потребителей: Защищенные хозяйствующие субъекты в области технологий могут предложить более безопасные и качественные продукты и услуги. Когда компании имеют возможность контролировать свою интеллектуальную собственность, они могут гарантировать, что продукты, которые они предлагают, отвечают определенным стандартам и требованиям безопасности.

5. Региональное развитие: Защита хозяйствующих субъектов в области технологий может быть важна для экономического развития регионов. Когда компании, специализирующиеся на технологиях, защищены и получают прибыль от своих интеллектуальных активов, они могут создавать новые рабочие места и привлекать инвестиции в свою область.

В целом, защита хозяйствующих субъектов в области технологий способствует стимулированию инноваций, развитию конкуренции, обеспечению безопасности продуктов и услуг, а также экономическому развитию регионов.

Для защиты хозяйствующих субъектов в области информационной безопасности необходимо проводить следующие мероприятия.

1. Определить и оценить риски: провести анализ возможных информационных угроз, оценить их вероятность и потенциальные последствия для хозяйствующего субъекта.

2. Обеспечить защиту сетевой инфраструктуры: применить меры по обеспечению безопасности компьютерных сетей, такие как установка межсетевых экранов, антивирусное программное обеспечение, мониторинг активности сети и т.д.

3. Установить политику управления доступом: определить права доступа сотрудников к информации в соответствии с их ролями и обязанностями, а также мониторить и регулярно обновлять список уполномоченных пользователей.

4. Развивать план реагирования на инциденты: определить процедуры и ответственных лиц для оперативного реагирования на возможные инциденты информационной безопасности.

5. Проводить аудит информационной безопасности: периодически проверять соответствие информационной безопасности требованиям и обнаруживать уязвимости и потенциальные риски.

6. Сотрудничать с внешними специалистами: при необходимости заключать договоры с компаниями, специализирующимися на информационной безопасности, для консультаций и проведения проверок.

7. Необходимо так же установить систему резервного копирования: регулярно создавать резервные копии важной информации и хранить их в отдельном месте, чтобы минимизировать потерю данных в случае инцидента.

8. Постоянно следить за новыми угрозами и техническими средствами защиты: держаться в курсе последних тенденций в области информационной безопасности и адаптировать защитные меры в соответствии со сменой угроз.