КИБЕРБЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

В эпоху глобальной цифровизации информационно-коммуникационные технологии (ИКТ) играют ключевую роль в трансформации общественных отношений, постепенно вытесняя традиционные механизмы государственного управления.

С одной стороны, ИКТ значительно оптимизируют организационные процессы, сокращая временные, финансовые и кадровые издержки. Они также способствуют повышению качества и доступности предоставляемых услуг. Кроме того, ИКТ формируют основу для комплексного сбора и обработки персональных, коммерческих и государственных данных, что требует строгого соблюдения норм законодательства Российской Федерации.

Однако, стремительное развитие цифровых технологий создает новые вызовы в области обеспечения информационной безопасности. Цифровизация общественных процессов способствует росту преступности в киберпространстве, что требует разработки и реализации комплексных мер по противодействию цифровой преступности. В этой связи, деятельность правоохранительных органов, направленная на борьбу с киберугрозами, становится приоритетным направлением современной правоохранительной политики.

В условиях активного развития информационных и коммуникационных технологий (ИКТ) особое значение приобретает обеспечение информационной безопасности. Для минимизации рисков, связанных с киберугрозами, рекомендуется соблюдать следующие меры предосторожности:

1. Разработка сложных паролей. Пароли должны быть достаточной длины и содержать комбинацию строчных и прописных букв, цифр и специальных символов. Не допускается использование идентичных паролей для различных учетных записей.

2. Критическая оценка электронной корреспонденции. Рекомендуется воздержаться от открытия писем, полученных от неизвестных отправителей, поскольку они могут представлять собой попытки фишинга или распространения вредоносного программного обеспечения.

3. Анализ гиперссылок. Следует проявлять осторожность при взаимодействии с веб-ссылками, особенно если их адреса вызывают подозрения. Рекомендуется осуществлять проверку веб-ресурсов на основании доменного имени, наличия SSL-сертификата и пользовательских отзывов.

4. Избегание использования открытых Wi-Fi сетей. Подключение к незащищенным Wi-Fi сетям в общественных местах может привести к несанкционированному перехвату сетевого трафика и компрометации учетных данных.