**Барабинская транспортная прокуратура информирует**

**Правовые механизмы и технологии противодействия преступности в сфере информационных технологий**

Целью правового регулирования отношений, связанных с применением и существующих и перспективных ИТ, при решении задач социально — экономического развития, повышения эффективности государственного управления, а также обеспечении информационной безопасности РФ, в том числе, и в сфере правоохранительной деятельности, является создание эффективной правовой основы реализации прав граждан, защиты общественных и государственных интересов в указанной сфере. Достижение этой цели требует координации и согласованности правотворческой деятельности органов власти, ее соответствия государственной политике РФ в сфере развития и использования ИТ и должно осуществляться по следующим направлениям:  
  
принятие новых законодательных и иных нормативных правовых актов, заполняющих пробелы в регулировании; – внесение изменений и дополнений в действующие законодательные и иные нормативные правовые акты с учетом состояния развития ИТ; – участие в выработке международно-правовых документов (включая межгосударственные соглашения) в сфере информационных технологий. Важность совершенствования законодательства определяется быстрым развитием в области ИТ и подчеркивает актуальность обеспечения высокого уровня информационной безопасности и защиты информации.  
В Российском Уголовном Кодексе существует глава 28, посвящённая преступлениям в сфере компьютерной информации «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 02.08.2019) [1]. Статья 272. Неправомерный доступ к компьютерной информации (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)  
  
Статья 273. Создание, использование и распространение вредоносных компьютерных программ (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)  
  
Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (введена Федеральным законом от 26.07.2017 N 194-ФЗ)  
В настоящее время для противодействия преступности в сфере информационных технологий требует неотложного совершенствования и развития действующей системы борьбы с киберпреступностью как целостной, интегрированной структуры, объединяющей противодействие киберпреступности на всех направлениях, включая и новое его проявление. Назовём некоторые способы борьбы с киберпреступниками: 1) Одним из инструментов противодействия кибермошеничеству является уголовно-правовой институт как в рамках национального законодательства, так и на уровне международном. В условиях борьбы с преступностью в интернет-сфере особую значимость приобретает предупредительная функция уголовно-правовой системы. 2) Другим эффективным путем самозащиты личной информации является правильное использование надежного антивирусного ПО. 3) Следующим механизмом борьбы с кибермошенниками можно назвать правоохранительные органы, которые если обнаруживают сайты с террористической или экстремистской информацией, то они связываются с провайдером, предупреждают его и просят принять меры, ограничивающие доступ к подобной информации.