Прокуратура Промышленного района г. Самара разъясняет

Противодействие преступлениям в сфере информационно-телекоммуникационных технологий (ИТТ) в Российской Федерации: правовые основы и актуальные меры

Введение

С развитием цифровых технологий растет и количество преступлений в сфере информационно-телекоммуникационных технологий (ИТТ). В Российской Федерации данная проблема регулируется комплексом нормативных актов, направленных на защиту информационной безопасности, персональных данных, финансовых активов и критической инфраструктуры. Основу правового регулирования составляют Уголовный кодекс РФ, федеральные законы и подзаконные акты, устанавливающие ответственность за киберпреступления и меры их предупреждения.

1. Правовые основы противодействия преступлениям в сфере ИТТ

1.1. Уголовная ответственность за киберпреступления

Основные составы преступлений в сфере ИТТ закреплены в Уголовном кодексе РФ (УК РФ):

- Статья 272. Неправомерный доступ к компьютерной информации

Наказывается доступ к информации, хранящейся на электронных носителях, если это повлекло ее уничтожение, блокирование, модификацию или копирование.

- Статья 273. Создание, использование и распространение вредоносных программ

Предусматривает ответственность за разработку и распространение вирусов, троянов и иного вредоносного ПО, способного нанести ущерб данным или системам.

- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации

Касается случаев, когда ненадлежащее использование ИТ-систем приводит к утечке или уничтожению данных.

- Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру (КИИ)

Введена в 2017 году и устанавливает строгую ответственность за атаки на объекты КИИ (госорганы, банки, энергетику, транспорт и др.).

- Статья 159.6. Мошенничество в сфере компьютерной информации

Касается хищения денежных средств или иного имущества с использованием IT-технологий (фишинг, кардинг, взлом аккаунтов).

1.2. Административная и гражданско-правовая ответственность

Помимо уголовного преследования, нарушения в сфере ИТТ могут повлечь:
- Административные штрафы по КоАП РФ (ст. 13.11 – нарушение защиты персональных данных, ст. 13.12 – несоблюдение требований к защите информации).
- Гражданские иски о возмещении ущерба (**ГК РФ, ст. 151.1 – компенсация за нарушение неприкосновенности частной жизни в интернете**).

2. Законодательные меры по профилактике киберпреступлений

2.1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Регулирует вопросы обработки и распространения данных.
- Обязывает операторов информационных систем обеспечивать их безопасность.

2.2. Федеральный закон от 26.12.1995 № 208-ФЗ «О безопасности критической информационной инфраструктуры»
- Устанавливает требования к защите объектов КИИ.
- Обязывает компании внедрять системы мониторинга и реагирования на кибератаки.

2.3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
- Регламентирует сбор, хранение и обработку персональных данных.
- Требует от организаций использовать сертифицированные средства защиты.

2.4. Регулирование интернет-пространства
- Закон о «суверенном интернете» (№ 90-ФЗ от 01.05.2019) – обеспечивает устойчивость российского сегмента сети.
- Закон о блокировке запрещенного контента (№ 476-ФЗ от 30.12.2020) – позволяет оперативно ограничивать доступ к сайтам с противоправной информацией.

3. Актуальные изменения в законодательстве (2023–2024 гг.)
В последние годы законодательство в сфере ИТТ активно ужесточается:

- Усиление ответственности за утечки данных (поправки в ст. 13.11 КоАП РФ).
- Обязательная идентификация пользователей соцсетей (закон о «цифровых профилях»).
- Борьба с фейками и кибермошенничеством (новые составы в УК РФ).
- Развитие системы киберпатрулирования (сотрудничество Роскомнадзора и МВД).

Заключение

Российское законодательство в сфере противодействия IT-преступлениям продолжает развиваться, реагируя на новые вызовы цифровой эпохи. Эффективная борьба с киберпреступностью требует не только жестких мер со стороны государства, но и повышения цифровой грамотности населения.

Соблюдение норм информационной безопасности – залог защиты от киберугроз.