

Преступления в сфере информационных технологий

В 21 веке информационные технологии стали неотъемлемой частью современной жизни, что не могло не сказаться на характере преступности, которая приобрела новые качества: техническую вооруженность, криминальный профессионализм, транснациональность. При этом все большее распространение получили преступления в сфере информационно-телекоммуникационных технологий.

Такие преступления включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду, и т. п.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Одним из наиболее распространенных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в том числе, сети Интернет, является мошенничество.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа преступного посягательства предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации (киберпреступления), которые на практике нередко используются в качестве инструментария завладения чужим имуществом. В целях борьбы с компьютерной преступностью в УК РФ предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния, как: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ).

Самый распространенный вид киберпреступлений в Российской Федерации — это телефонное мошенничество, при котором мошенники звонят по

телефону и пытаются узнать у владельцев банковских карт конфиденциальные данные, сделать перевод или установить программы удаленного доступа. Технология основана на использовании психологических слабостей человека и является достаточно эффективной. Преступник под видом сотрудника службы поддержки или службы безопасности банка звонит человеку, являющемуся пользователем банковской карты, после чего, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом ввиду его блокировки, узнает пин-код и иные данные, позволяющие получить доступ к банковскому счету потенциального потерпевшего.

Распространены также дистанционные хищения, совершаемые посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение.

Денежные средства неправомерно списываются со счетов потерпевших и тогда, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами.

Конфиденциальную информацию позволяет получить применение технологии фишинга. Зачастую злоумышленники рассылают потерпевшим под видом официальных писем, содержащие ссылки на фальшивые веб-страницы с формами для ввода необходимых преступникам данных, которые в последующем используются, в том числе, для доступа к банковским счетам граждан.

Данный способ является эффективным, поскольку многие пользователи, не раздумывая, открывают вложения или гиперссылки.

В связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью, преступления в сфере информационно-коммуникационных технологий становятся все более актуальными.

В целях предупреждения и пресечения указанных видов преступлений необходимо быть предельно внимательными при осуществлении банковских операций с использованием сети Интернет и мобильных телефонов, перепроверять полученную информацию, повышать уровень правовой, финансовой и компьютерной грамотности.