

Германова Анна Михайловна

магистрант

Научный руководитель

Шалагин Антон Евгеньевич

канд. юрид. наук, доцент, начальник кафедры

ФГКОУ ВО «Казанский юридический институт МВД РФ»

г. Казань, Республика Татарстан

ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

***Аннотация:** в статье рассматриваются приоритетные направления предупреждения мошеннических действий, предложены меры, направленные на предупреждение и минимизацию преступлений с использованием информационно-телекоммуникационных технологий, особое внимание обращено на деятельность правоохранительных органов по пресечению дистанционных преступлений.*

***Ключевые слова:** информационно-телекоммуникационные технологии, пресечение преступлений, профилактика преступлений, общесоциальные предупредительные меры, специальные предупредительные меры.*

Криминологическая ситуация в России остается сложной, поэтому предупреждению преступлений уделяется особое внимание. Государственными органами и структурами принимаются необходимые меры по изменению сложившейся ситуации и снижению напряженности в данной сфере.

Основной целью деятельности, направленной на предупреждение преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, является снижение уровня такого вида преступлений, а также защита личности, общества и государства от преступных посягательств.

Основная задача предупреждения преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, состоит в выявлении, устранении и нейтрализации причин и условий, способствующих совершению названных преступлений и предотвращении готовящихся преступлений.

Практическая реализация целей, задач предупреждения преступлений напрямую зависит от правоприменительной деятельности, объектом которой выступает система причин и условий, способствующих совершению преступлений, что дает основание рассматривать предупредительную деятельность как целенаправленную деятельность государства, общества, физических и юридических лиц, направленную на недопущение их совершения путем выявления, анализа, устранения или нейтрализации причин преступлений, условий, способствующих их совершению, оказания предупредительного воздействия на лиц с противоправным поведением.

Предупреждение преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, требует весьма серьезных усилий государства и общества и может быть успешным только на основе использования широкого комплекса общесоциальных и специальных предупредительных мер.

При этом общесоциальное предупреждение включает в себя совершенствование экономических, социальных, духовных, политических отношений в обществе; выявление и устранение диспропорций в них; криминологическая экспертиза; экспертные исследования, укрепление законности, социальная защита населения. На этом уровне наиболее эффективным является разработка социальных программ по отдельным проблемам криминогенного характера.

Основой обще социального уровня предупредительной деятельности названных преступлений должны стать результаты проведенного мониторинга современного состояния цифровой преступности, при этом должны учитываться не только показатели зарегистрированных преступлений, совершенных в сфере цифровых технологий, но и реальное состояние с учетом ее латентной части, причинного комплекса, судебной-следственной практики по данной категории

дел, механизма привлечения к уголовной ответственности и его реализация в целом, социально политической и экономической ситуации, сложившейся на момент подготовки мер предупредительного воздействия, результаты криминологического прогноза на краткосрочный и среднесрочный периоды, и другие составляющие, которые позволят правильно и в полном объеме учесть все необходимые особенности современных криминологических угроз с целью определения направления предупредительного воздействия.

Специально-криминологическое предупреждение заключается в деятельности по предотвращению, пресечению и раскрытию преступлений; выявлению и устранению (нейтрализации) детерминант преступности, причин и условий конкретных преступлений; оздоровления социальной микросреды, коррекции поведения лиц, исправлению лиц, от которых можно ожидать совершения или уже совершивших преступления.

Социально-политические меры предупреждения преступлений, совершаемых в сфере информационно-телекоммуникационных технологий являются основными при осуществлении названной деятельности, так как государственная уголовная политика во «многом зависит от укрепления роли государственной власти, рационализации подходов к выработке решений в формировании уголовной политики, от создания условий для эффективной работы механизмов, основанных на саморегулировании и препятствующих развитию дестабилизирующих факторов». Важным направлением в данном случае должны стать меры, направленные на стабилизацию политической ситуации в России; укрепление и повышение авторитета политической власти; создание законодательной базы по охране цифровых технологий и защиты, но базы правовой защищенности российских граждан; выработка стратегии и тактики уголовной политики, а также политики идеологического воздействия.

К социально-экономическим мерам предупреждения преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, следует отнести укрепление кредитно-денежной системы государства, оздоровление экономики, укрепление мер социальной защиты населения

Особое внимание следует уделить и нормативным предписаниям, регламентирующим противодействие цифровой преступности, в соответствии с международно-правовыми стандартами и международными обязательствами России; заключение и ратификация международных Конвенций, межгосударственных договоров и соглашений по вопросам противодействия цифровой преступности.

повышению профессионализма субъектов предупредительной деятельности в сфере информационно-телекоммуникационных технологий. В связи с этим необходима подготовка и переквалификация сотрудников правоохранительных органов, необходимо укрепление подразделений, которые непосредственно осуществляют мероприятия по противодействию преступлениям в сфере цифровых технологий.

Субъектами предупреждения преступности с использованием информационно-телекоммуникационных технологий являются федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, действующие в пределах своей компетенции как непосредственно, так и через подведомственные им структуры. Стоит отметить, что основная работа сотрудников правоохранительных органов должна заключаться, прежде всего, в доведении до граждан элементарных правил безопасности, таких как недопустимость:

- загрузки из сети Интернет программных продуктов из непроверенных источников; перехода по рекламным ссылкам в интернете, сулящим бесплатные услуги, различные призы или существенные скидки; просмотр корреспонденции от неизвестных адресатов; несвоевременное обновление программного обеспечения;
- общения в социальных сетях с незнакомыми пользователями, за которыми могут скрываться мошенники, сектанты, вербовщики в террористические организации;
- покупки SIM-карт с рук или оставление своих паспортных данных сомнительным «конторам»;

- отправки денежных переводов лицам, предлагающим посреднические услуги в разрешении проблем с родственниками, знакомыми, якобы попавшими в беду;

- передаче данных с кредитных или дебетовых карт, пользовательских паролей и кодовых слов, запрашиваемых по телефону или через социальные сети от лица друзей, знакомых, кредитных или иных организаций под различными предложениями;

- указания в своем профиле социальной сети личной информации, в том числе о своем образе жизни, планируемых отъездах и т. п.;

- проведения операций в интернет-банкинге без проверки истинности адреса личного кабинета или при наличии дополнительных, не предусмотренных стандартной процедурой, запросов (защита от «фишинга»);

- непринятия срочных мер по блокированию кредитных или дебетовых карт при получении СМС о несанкционированном списании или переводе средств третьим лицам;

- регистрации в личных кабинетах, на Интернет-ресурсах или онлайн-магазинах с простыми паролями, состоящими из нескольких цифр, коротких слов, соседних клавиш на клавиатуре, личных памятных дат, адресов или номеров телефонов;

- записей личных паролей на стикерах, приклеенных к монитору, или в других легкодоступных местах.

Таким образом, можно говорить о том, что предупреждение преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, требует серьезных усилий как государства, так и общества.

Список литературы

1. Артимович, Д. А. Искусство цифровой самозащиты / Д. А. Артимович. – Москва : АСТ, 2023. – 224 с.

2. Ищук Я.Г. Цифровая криминология : учеб. пособие / Я.Г. Ищук, Т.В. Пинкевич, Е.С. Смольянинов. – Москва: Академия управления МВД России, 2021. – 244 с.

3. Криминология. Особенная часть : учебник для курсантов и слушателей образовательных организаций высшего образования системы МВД России / А. Е. Шалагин, Р. Р. Абдулганеев, О. В. Артюшина [и др.] ; под общ. ред. Ф.К. Зиннурова. – 2-е изд., перераб. и доп. – Казань : Казанский юридический институт Министерства внутренних дел Российской Федерации, 2016. – 524 с.

4. Ларина, Е. С. Криминал будущего уже здесь / Е. С. Ларина, В. С. Овчинский. – Москва : Книжный мир, 2017. – 480 с.

5. Профилактика преступлений: отечественный и зарубежный опыт : учебное пособие / Ф. К. Зиннуров, А. Е. Шалагин, Р. Р. Абдулганеев [и др.]. – Казань : Казанский юридический институт Министерства внутренних дел Российской Федерации, 2023. – 218 с.

6. Соловьев, И. Н. Как не стать жертвой мошенников и пособником преступников : пособие для подростков и их родителей / И. Н. Соловьев. – Москва : Проспект, 2026. – 56 с.

7. Шалагин, А. Е. Криминология и предупреждение преступлений / А. Е. Шалагин. – Москва : Юрлитинформ, 2021. – 240 с.

8. Чекунов, И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : автореф. дис. / И. Г. Чекунов. – Москва, 2013