УДК 004.056

Правовые механизмы профилактики и пресечения киберпреступности в субъектах Российской Федерации (на примере Республики Ингушетия)[1]

Евлоев Абдул-Малик Дзауриевич, магистрант, Московский государственный университет имени М. В. Ломоносова, evloev.abdul-malick@yandex.ru

В статье рассматриваются ключевые аспекты киберпреступности, существующие правовые механизмы борьбы с данной угрозой и особенности ее проявления на примере Республики Ингушетия. Анализируется текущая ситуация в регионе с примерами финансовых мошенничеств, атак на государственные порталы и взломов учетных записей, а также предлагаются пути совершенствования систем безопасности. Особое внимание уделено роли правоохранительных органов в расследовании и предупреждении киберпреступлений, возможным мерам по повышению уровня цифровой грамотности на федеральном и региональном уровнях.

Ключевые слова: информационная безопасность, киберпреступность, цифровизация, правовые механизмы, кибератаки, финансовое мошенничество.

В современном мире вопрос информационной безопасности становится все более актуальным. С ростом уровня цифровизации мы получаем массу преимуществ — быстрый доступ к услугам, удобные электронные сервисы, возможности дистанционного обучения и работы. Однако наряду с этим общество сталкивается с новыми угрозами, среди которых особенно опасной является киберпреступность.

Республика Ингушетия, являясь частью Российской Федерации, активно развивается в сфере цифровых технологий. В регионе внедряются электронные госуслуги, модернизируются различные информационные системы, появляются новые онлайн-сервисы для граждан. Однако эти позитивные изменения одновременно делают регион уязвимым перед киберугрозами.

К сожалению, еще не все жители хорошо ориентируются в цифровом пространстве, а у правоохранительных органов нередко не хватает ресурсов и опыта для противодействия сложным кибератакам. В данной работе рассматривается проявление киберпреступности в Республике Ингушетия, анализируются правовые инструменты для противодействия этому явлению, а также исследуется роль полиции и других силовых ведомств в защите информационной сферы региона.

В мире и в России киберпреступность продолжает набирать обороты. Злоумышленники активно используют возможности анонимности в сети для совершения различных махинаций: мошенничества, кражи данных, атак на государственные системы и т. д.

Число преступлений, совершенных с использованием информационных технологий, по данным МВД России, увеличилось с 174 тыс. в 2021 г. до 500 тыс. в 2023 г. Наиболее распространенные виды киберпреступлений включают:

1) мошеннические схемы (фальшивые сайты, фишинг, обман через соцсети);

2) распространение и использование вирусных программ (вымогатели, шпионские приложения);

3) атаки на государственные учреждения (доступ к секретным данным, отключение важных ресурсов);

4) преступления с криптовалютами (мошенничество, создание финансовых пирамид, незаконный майнинг).

В Северо-Кавказских республиках, включая Ингушетию, киберпреступления также становятся все более актуальными. По данным МВД, только за 2020 г. число таких преступлений в регионе увеличилось на 23 %. В регионе наиболее часто фиксируются:

1) телефонные мошенничества, когда преступники представляются сотрудниками банков или других организаций;

2) взломы личных страниц в соцсетях с целью шантажа или распространения ложной информации;

3) атаки на официальные веб-сайты органов власти региона.

В Ингушетии ситуация усложняется рядом факторов:

— низкий уровень знаний об информационной безопасности у части населения;

— недостаточно развитая техническая база у правоохранительных органов, что приводит к передаче сложных дел на федеральный уровень;

— необходимость модернизации существующих государственных информационных систем, чтобы повысить их защиту.

Часто злоумышленники звонят жителям республики, представляясь сотрудниками банков и выманивая конфиденциальные данные. В 2023 г. была разоблачена группа мошенников, создававших фальшивые сайты известных интернет-магазинов, которые похитили более 5 млн руб. у жителей региона.

Взлом личных аккаунтов. Другой распространенный вид преступлений — это взлом страниц в соцсетях. Например, в 2022 г. неизвестные взломали страницу одного местного общественного деятеля, публикуя от его имени ложную информацию, что нанесло ущерб его репутации.

Атаки на государственные порталы. В 2022 г. была зафиксирована попытка взлома портала госуслуг Республики Ингушетия. Специалисты быстро отреагировали и предотвратили утечку данных, но инцидент показал, что региональные информационные ресурсы остаются под угрозой.

Правовые механизмы пресечения киберпреступлений. В России существует несколько основных законов, регулирующих ответственность за киберпреступления и меры по их предотвращению:

Уголовный кодекс РФ:

— ст. 272 «Неправомерный доступ к компьютерной информации»;

— ст. 273 «Создание, использование и распространение вредоносных программ»;

[1] Научный руководитель: Морозов Андрей Витальевич — профессор кафедры компьютерного права и информационной безопасности, Московский государственный университет имени М. В. Ломоносова, доктор юридических наук, профессор.

— ст. 274 «Нарушение правил эксплуатации информационных систем».

Федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» — регулирует защиту важнейших информационных систем страны.

Федеральный закон N 149-ФЗ «Об информации, информационных технологиях и о защите информации» — устанавливает общие правила обращения с информацией и меры по ее защите.

В Ингушетии также предпринимаются усилия для повышения уровня кибербезопасности, включая:

1. Образовательные проекты. В школах и вузах проводятся семинары и лекции по защите личных данных.

2. Сотрудничество с федеральными ведомствами. Регион активно обменивается опытом с Роскомнадзором и ФСБ для более оперативного реагирования на возможные кибератаки.

3. Профилактические меры. Сотрудники МВД регулярно информируют граждан о мошеннических схемах и дают советы, как избежать интернет-уловок.

В МВД Республики Ингушетия работают специалисты, занимающиеся цифровой криминалистикой. Они анализируют следы, оставляемые преступниками в сети, и пытаются выявить виновных.

Сотрудники правоохранительных органов проводят просветительские акции, публикуют материалы в СМИ, объясняя, как избежать мошенничества в интернете и какие меры безопасности нужно соблюдать.

Для эффективной борьбы с кибератаками сотрудники правоохранительных органов проходят специализированные курсы и тренинги, чтобы быть в курсе новых технологий и методов борьбы с интернет-преступностью.

Несмотря на достигнутые успехи, в борьбе с киберпреступностью в Ингушетии все еще остаются серьезные проблемы:

1. Нехватка специалистов. Остро ощущается дефицит подготовленных кадров, способных профессионально расследовать сложные киберпреступления.

2. Ограниченные финансовые ресурсы. Недостаток средств для регулярного обновления систем защиты и обеспечения правоохранительных органов современным оборудованием.

3. Старая инфраструктура. Устаревшая инфраструктура. Локальные сети и серверы требуют модернизации для соответствия актуальным стандартам кибербезопасности.

Чтобы улучшить ситуацию, необходимо:

1. Создавать в регионе обучающие центры по кибербезопасности для подготовки новых специалистов.

2. Продолжать развивать взаимодействие с федеральными структурами, которые обладают большим опытом и ресурсами.

3. Разрабатывать и внедрять программы по защите важной инфраструктуры на местном уровне, учитывая специфику региона.

Таким образом, киберпреступность — серьезная проблема, затрагивающая как весь мир, так и отдельные регионы России, в том числе Республику Ингушетия. Рост числа атак и их сложность требуют от государства и общества применения современных технологий и более широких просветительских мероприятий.

Только при совместной работе разных уровней власти, вовлечении правоохранительных органов, IT-специалистов и самих граждан удастся добиться стабильной информационной безопасности. Главное — повышать осведомленность людей, развивать необходимые навыки и укреплять инфраструктуру, чтобы эффективно противостоять любым киберугрозам.

Примечания

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства РФ. 1996. N 25. Ст. 2954.
2. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 2017. N 167.
3. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. N 165.

English version

Legal mechanisms for the prevention and suppression of cybercrime in the subjects of the Russian Federation (the case of the Republic of Ingushetia)

Evloev Abdul-Malik Dzaurievich, master’s student, Lomonosov Moscow State University

This article examines the key aspects of cybercrime, existing legal mechanisms for combating this threat, and its manifestations, focusing on the Republic of Ingushetia. The current situation in the region is analyzed, with examples of financial fraud, attacks on government portals, and account hacking, as well as proposals for improving security systems. Special attention is given to the role of law enforcement agencies in investigating and preventing cybercrimes, as well as potential measures to enhance digital literacy at the federal and regional levels.

Keywords: information security, cybercrime, digitization, legal mechanisms, cyberattacks, financial fraud.