Феномен киберпреступности в современной России – актуальные проблемы и пути решения

Научный руководитель – Абдрахманова Елена Робертовна

Шведкин Данила Андреевич

Студент (бакалавр) Ульяновский государственный университет, Ульяновск, Россия

E-mail: dshvedkin03@mail.ru

Современная Россия, следуя общемировым прогрессивным тенденциям и стратегиям, в числе бескрайнего множества сфер активно развивает сферу информационных технологий. Им свойственно постоянное модифицирование, возрастает их доступность и удобство для широкого круга пользователей, что неизбежно приводит к их внедрению в сферы не только общественной жизни, но и в механизм функционирования государственной машины. Бытует мнение, что чем более государство развито, тем активнее в нем протекают процессы цифровизации. Несомненно, в этом имеется множество положительных моментов, однако стоит рассмотреть и иную сторону медали. Сам процесс цифровизации, активный рост технологий, множественные инновационные достижения могут знаменовать собой различного характера риски и угрозы, поскольку информационными технологиями как орудием, средством совершения своих преступных деяний пользуются криминальные элементы общества. Правонарушители во многих случаях намного быстрее правоохранителей постигают технологии, а также адаптируются к изменчивым условиям, что дает им новые рычаги в достижении своих противоправных целей. Стремительный прогресс в развитии информационных технологий и процессы цифровизации и без того усугубляют проблемы, связанные с противодействием преступности. С уверенностью можно сказать, что на сегодняшний день от рук преступников, орудующих в виртуальном пространстве, могут пострадать не только отдельно взятые люди, но и целые государства. К тому же, безопасность десятков тысяч человек может находиться в прямой зависимости всего от одного или нескольких преступников. Очевидно, что количество киберпреступлений возрастает пропорционально числу клиентов и пользователей компьютерных сетей, то есть настоящий период характеризуется постоянным ростом компьютерных преступлений. Представляется, что тенденция к увеличению компьютерной преступности наблюдается ввиду дефицита мощных инструментов контроля со стороны государственных структур. При этом стоит сказать, что официальная статистика о состоянии компьютерных преступлений в России весьма мало информативна ввиду крайне высокой

латентности подобных деяний, и оперировать какими-либо конкретными цифрами бесполезно.

Важным моментом здесь является то, что в нормах Уголовного кодекса РФ не содержится какой-либо дефиниции «киберпреступления». Угловно-правовые нормы содержат составы информационных преступлений, где отражаются вопросы преступного использования информационных технологий или средств компьютерной техники. Именно поэтому сфера киберпреступности в данный момент не находит своего законодательного регулирования в России, хотя она имеет приоритетное положение в осуществлении уголовно-правовой политики государства. Важно сказать, что до недавнего времени термин «компьютерная преступность» обозначал любое преступное деяние против компьютерной техники, сетей или с использованием компьютеров в качестве орудия совершения этого деяния. Однако с развитием уголовной доктрины стало очевидно, что эти преступления совершаются и с использованием других цифровых устройств, например, смартфонов, ввиду чего стало применяться понятие «киберпреступность».

Разграничение понятий «киберпреступление» и «информационное преступление, преступление в сфере компьютерной информации» можно провести, в первую очередь, с помощью объекта и предмета данных преступных посягательств. Объектом компьютерных, информационных преступлений выступают общественные отношения, возникающие по обеспечению целостности и доступности электронной информации, а также сохранности компьютерных средств, необходимых для ее обработки, а предмет представлен средствами хранения, обработки или передачи компьютерной информации. Объект и предмет киберпреступлений гораздо обширнее. По объекту посягательства можно выделить несколько разновидностей киберпреступлений – экономические, против личности и неприкосновенности частной жизни, а также против общественной безопасности и общественного порядка и другие. Предметом рассматриваемых преступных посягательств может выступать виртуальная информация, находящаяся в Интернете. То есть можно сказать, что киберпреступность охватывает всю массу деяний в сфере информационных технологий, а также имеет свои отличительные признаки, характеристики, особенности, что опять же, лишь аргументирует необходимость соответствующего законодательного регулирования.

В доктрине же феномен киберпреступности давно разрабатывается и изучается. Компонуя множество мнений и теорий можно сказать, что юридическая литература характеризует киберпреступления как преступную деятельность, совершение которой направлено на неправомерное

использование компьютерной техники, компьютерной сети или сетевого устройства. Субъектами киберпреступлений выступают отдельные лица (хакеры) или даже целые организации, обладающие более углубленными по сравнению с обычными людьми знаниями и навыками в сфере использования компьютерных технологий, либо обладающие специализированным техническим оборудованием или иными ресурсами, предоставляющими доступ к более широким возможностям использования цифровых технологий, при помощи которых они скрывают следы преступлений, долгое время оставаясь непойманными. Именно по этой причине киберпреступники не ограничиваются одним преступным деянием, совершая регулярно десятки преступлений однородного характера, что лишь увеличивает общественную опасность данных лиц.

Киберперступность приобрела характер серьезной международной проблемы, поэтому она не остается без внимания и российских правоохранителей. Перечень способов совершения таких преступлений весьма разнообразен ввиду того, что компьютерное пространство обладает рядом особенностей, позволяющих значительно затруднить механизмы привлечения к ответственности, чему также способствует постоянное развитие IT – технологий. Так, киберпреступление не имеет географических пределов, ввиду чего может быть совершено в одной стране или ее территориальном субъекте против другой страны. Также, в преступлениях цифрового характера правонарушители зачастую не оставляют физических следов, но оставляют за собой цифровой след, поскольку феномен киберпреступлений тесно связан с пространством, симулируемым и опосредованном различными электронными устройствами, имеющими развитые механизмы анонимности. Следует отметить и дистанционный характер данных преступных деяний при отсутствии непосредственного физического контакта преступника с потерпевшим. Самое главное – это невозможность предотвратить, пресечь преступление данного вида с помощью традиционных методов и средств.

Итак, к числу наиболее распространенных киберпреступлений относятся кардинг – разновидность мошенничества с использованием платежных карт, спаминг (мошенничество, связанное с массовой рассылкой рекламы, содержащей вирусные компоненты, лицам, которые не давали своего добровольного согласия на ее получение), фишинг - получение обманным путем личных данных пользователя - логина, пароля, номера телефона, банковской карты, фарминг - автоматическое перенаправление пользователей на ложные сайты (точные копии сайтов реальных банков, торговых площадок и др.) с целью хищения данных или денежных средств, и хакинг - выявление уязвимых, незащищенных областей какой-либо информационной системы с целью получения доступа к ней. Очень частым

явлением в киберпространстве является совершение информационных атак, краж, а также заключение сделок, связанных с незаконной торговлей людьми, оружием и наркотическими и иными запрещенными веществами.

Конечно, нельзя сказать, что ответственность за совершение киберпреступлений вовсе не отражена в российском законодательстве. Так, в ст. 17 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.03.2023) установлена ответственность дисциплинарного, административного, гражданско-правового и уголовного характера за несоблюдение требований в сфере информационной безопасности. В уголовном законе ответственность за преступления в сфере компьютерной информации регламентируется главой 28, в которую включены 5 статей. Помимо этого, Указом Президента Российской Федерации от 5 декабря 2016 г. №646 была утверждена Доктрина «Об информационной безопасности Российской Федерации», где нашли свое отражение главные информационные угрозы, силы, меры, средства информационной безопасности государства, а также определены основные направления и стратегические задачи в сфере обеспечения информационной защищенности с учетом государственных приоритетов государства. Однако стоит понимать, что с каждым новым днем вопрос о более глубокой разработке положений, касающихся рассматриваемых правонарушений, а также мер превенции и способов борьбы с ними приобретает все большую необходимость.

Цели совершения киберпреступлений разнообразны. Это может быть нанесение политического. экономического, морального, идеологического, культурного и другого вреда людям или организациям с помощью различных технических средств, имеющих доступ к сети Интернет. Более того, феномен киберперступности в процессе своего развития постепенно приобрел характер угрозы национально-государственной, поскольку зачастую цели, преследуемые преступниками – подрыв основ государственного и общественного строя, национальной безопасности, дестабилизация общественности конкретно взятой страны. Поэтому в доктрине уголовного права все чаще говорят о кибертерроризме как одной из форм киберпреступлений.

Феномен киберпреступности носит масштабный и противоречивый характер, борьба с ним требует тесного сотрудничества различных спецслужб и органов. Для проведения более эффективной политики по борьбе с киберпреступлениями и, в том числе, с информационными преступлениями, могут быть предприняты следующие меры:

1) совершенствование технологий, содействующих выявлению киберпреступлений, а также способов проведения расследований данных правонарушений

2) разграничение понятий «киберпреступление» и «преступления в сфере компьютерной информации» на законодательном уровне

3) ужесточение ответственности за совершение преступлений, описанных в гл. 28 УК РФ, вплоть до категории особо тяжких

4) введение новых положений, касающихся уточнения в уголовном законе конкретных киберпреступлений ввиду их повышенной опасности

5) целенаправленная борьба с кибертерпреступностью в различных ее формах и проявлениях

Литература:

1. Христинина, Е.В. К вопросу об уголовно-правовом противодействии киберпреступности / Е. В. Христинина // Вестник Сибирского юридического института МВД России. – 2021. № - 4(45). – С. 150-154.
2. Шарков, Ф. И. Цифровые технологии: преимущества, проблемы развития и киберпреступность / Ф. И. Шарков, И. С. Омельчук // Коммуникология: электронный научный журнал. – 2021. - № 2. – С. 35-54.
3. Тимофеев, А. В. Киберпреступность как социальная угроза и объект правового регулирования / А. В. Тимофеев, А. А. Комолов // Вестник Московского государственного областного университета. Серия: Философские науки. – 2021. - № 1. – С. 95-101.