

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПНОСТИ

Д.А. Сычъ, курсант

Научный руководитель: И.Р. Аминов, канд. юрид. наук, доцент

Уфимский юридический институт МВД России
(Россия, г. Уфа)

DOI: 10.24412/2500-1000-2024-11-3-162-164

Аннотация. Статья описывает актуальную проблему в науке криминологии – появление нового объекта преступления, образующийся в сфере компьютерных и иных технологий, тем самым и возникновение новых общественных отношения в рассматриваемой сфере. В статье раскрывается целостное понятие киберпреступности, а также основные причины и условия, способствующие развитию киберпреступности как наиболее распространенного явления в современном цифровом обществе.

Ключевые слова: киберпреступность, глобализация, эволюция, интернет, экономическая преступность, информационные технологии.

В настоящих реалиях наиболее преуспевающая тенденция в современном обществе является компьютерные и IT-технологии. Действительно, тенденция проявляет себя с лучшей стороны, внедряясь практически во все сферы жизнедеятельности, упрощает и ускоряет многие процессы. Ни одно явление не обходится и без негативной составляющей, что присутствует и в данной тенденции – киберпреступность. Соответственно, имея негативный окрас, данное направление в науке уголовного права и криминологии создает новый объект и новые общественные отношения в сфере информационных и иных технологий, что является важным вопросом в государстве.

Актуальность данной темы подтверждается официальной статистикой Министерства внутренних дел Российской Федерации (далее – МВД РФ). Так, за 2021 год преступления, совершаемые с использованием информационных технологий, составили 517722, при этом пик таких преступлений приходится на Чеченскую Республику. В 2022 году таких преступлений насчитывается 522065 и регионы, где число таких преступлений преобладали – это Республика Северная Осетия – Алания, Чукотский автономный округ и Тверская область. В 2023 году таких преступлений насчитывается уже 676951, что на 77% больше предыдущего года, при этом стоит отметить следующие регионы РФ, имеющие наибольшее количество зарегистрированных преступлений в этой сфере – Ненецкий автономный округ, Республика Калмыкия и Нов-

городская область. На сегодняшний день с января по август 2024 года зарегистрировано уже 500389, что фактически регистрировалось в 2021-2022 гг., предполагаем, что рост преступлений значительно превысит и показатели 2023 года [3]. Можем сделать вывод о том, что развитие информационных технологий настолько же стремительно, как и число преступлений, совершающихся в рассматриваемой сфере. Соответственно встает вопрос о криминологической характеристике таких преступлений и мерах по их противодействию.

Киберпреступность, порождение эпохи глобализации, продолжает эволюцию вместе с развитием интернета и информационных технологий. Особенно популярным видом мошенничества, процветающим в бескрайних просторах сети, является фишинг. Этот термин происходит от английского «fishing», что подчеркивает суть действий мошенника – «вылавливание» конфиденциальной информации у пользователей под различными предлогами [1, с. 28]. Фишинговые атаки обычно осуществляются путем отправки электронных писем или создания веб-сайтов, которые на первый взгляд кажутся легитимными, но на самом деле предназначены для кражи личных данных, таких как пароли, номера банковских счетов, информация о кредитных картах и другие сведения, представляющие ценность для преступников.

Значение фишинга в контексте киберпреступности трудно переоценить. Этот метод не

только распространен из-за своей эффективности, но и потому, что он постоянно адаптируется к новым реалиям информационного общества, становясь всё более изощренным и трудно распознаваемым.

Киберпреступность является относительно новым, но стремительно развивающимся явлением, которое получило мощный толчок к развитию вместе с эволюцией интернета и информационных технологий. Это многогранное правовое явление, охватывающее различные виды незаконной деятельности, начиная от мошенничества и кражи персональных данных до кибератак на государственные учреждения. Глобализация и ускоренный обмен данными усилили эту тенденцию, делая традиционные методы борьбы с преступностью менее эффективными в контексте международного киберпространства.

Киберпреступность не знает границ, что делает ее особенно заманчивой для преступников, стремящихся извлечь выгоду из анонимности, предоставляемой интернетом. Информационные технологии, развиваясь, создают новые возможности для общества, но в то же время расширяют арсенал средств, доступных преступникам. Эта двойственность является ключевым фактором, делающим киберпреступность сложной для исследования и противодействия.

Особенностью киберпреступлений является их высокий уровень анонимности и трансграничность. Преступники могут совершать атаки, не выходя из своего дома, находясь в любой точке мира, что существенно затрудняет процесс их идентификации и привлечения к ответственности. Это усложняет работу правоохранительных органов и требует от них новых методов и подходов в борьбе с киберпреступностью.

Также киберпреступность характеризуется быстрой адаптацией к изменениям в информационных технологиях. Преступники быстро осваивают новые технологии и находят способы их использования в незаконных целях. Это делает киберпреступность чрезвычайно динамичным и развивающимся сегментом преступности.

Среди причин и условий возникновения такого преступного явления как киберпреступность выделяют основные: непосредственно сам процесс компьютеризации и ав-

томатизации (усовершенствование информационных технологий и расширение производств; виртуальных форм финансовых расчетов и платежей), а также уровень развития страны, то есть ее экономическая составляющая. Кроме этого, выделяют такие условия и мотивы как доступность, прибыльность и факт удаленности, которые благоприятно влияют на сложность раскрытия таких преступлений [4, с. 796].

Юридические меры играют весомую роль в противодействии и предупреждении преступности. Они охватывают почти все области, в том числе процесс криминализации, международное сотрудничество, законотворческий процесс и другое. Безусловно, как ранее уже отмечалось, что процесс компьютеризации влияет на возникновение новых общественных отношений с техникой, что порождает преступления и следствием этого является криминализация и пенализация как один способов противодействия киберпреступности на национальном и мировом уровне [2, с. 46-47]. В нашем государстве одним из видов противодействия выступает введение главы 28 в Уголовный кодекс Российской Федерации (далее – РФ). В данной мере имеются и свои минусы. Во-первых, такая преступность развивается очень стремительно, соответственно напрашивается следствие – органы государственной власти фактически не успевают на правовом уровне урегулировать новые формы преодоления противодействия преступлениям в киберпространстве и, как итог, отсутствуют необходимые меры для борьбы с таким видом преступности.

Силы государства не стоит недооценивать. Так или иначе на международном уровне между странами, с участием РФ в том числе, решаются многочисленные вопросы, направленные на снижение киберпреступности и установлении единых правовых мер.

Стоит отметить и криминологические исследования в данной области. Целью таких исследований выступают технологии, а именно какими способами злоупотребляют подобными информационными технологиями, чтобы создать программы или меры по нейтрализации такого злоупотребления, соответственно исключив детерминанты преступления. Такие исследования преследуют еще одну цель – оценка рисков при разработке и внед-

рении определенных технологий, чтобы на этапе внедрения иметь надежную систему защиты.

Помимо обозначенных выше мер противодействия киберпреступлений в рамках уголовной политики выделяют и другие: выработка концепции развития законодательства; стратегическое и тактическое планирование борьбы с преступностью, включая идеологические, социальные и воспитательные меры; правоприменение и регулярный мониторинг эффективности, но, к сожалению, в рамках данной статьи не представляется возможным рассмотреть все способы и элементы противодействия данному преступному явлению [2, с. 62].

Таким образом, можно сказать о том, что научно-технический прогресс непрерывен в своем развитии, также как и преступный мир, поэтому эти обе системы отражая на себе IT изменения должны находиться в определенном балансе, исходя из философии синергетики. Кроме того, постоянное совершенствование этих двух систем говорит нам о новых предпосылках обновления и совершенствования права (появление новых общественных отношений, регулируемых уголовным законодательством, новой усложненной терминологией и т.д.), что порождает необходимость соответствующей регламентации и быстрого реагирования.

Библиографический список

1. Завадский В.П. Проблемы организации борьбы с киберпреступностью // Материалы II Международной научно-практической конференции. – 2022. – С. 28-29.
2. Козаев Н.Ш. Противодействие злоупотреблениями современными технологиями: международно-правовые и уголовно-правовые аспекты // Монография. – М.: из-во: Юрлитинформ, 2019. – 177 с.
3. Краткая характеристика состояния преступности в Российской Федерации. – [Электронный ресурс]. – Режим доступа: <https://мвд.рф/reports/1/> (дата обращения: 25.09.2024).
4. Куленко К.Н. Проблемы киберпреступности в РФ и пути ее решения // Научное обеспечение агропромышленного комплекса. – 2023. – С. 796-797.

CRIMINOLOGICAL CHARACTERISTICS OF CYBERCRIME

D.A. Sych, Cadet

**Supervisor: I.R. Aminov, Candidate of Legal Sciences, Associate Professor
Ufa Law Institute of the Ministry of Internal Affairs of Russia
(Russia, Ufa)**

Abstract. *The article describes an urgent problem in the science of criminology – the emergence of a new object of crime, formed in the field of computer and other technologies, thereby the emergence of new social relations in the field under consideration. The article reveals the holistic concept of cybercrime, as well as the main causes and conditions contributing to the development of cybercrime as the most common phenomenon in modern digital society.*

Keywords: *cybercrime, globalization, evolution, Internet, economic crime, information technology.*