DOI 10.37882/2223-2974.2024.01.11

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КИБЕРПРЕСТУПЛЕНИЙ В РОССИИ И ЗАРУБЕЖНЫХ СТРАНАХ

COMPARATIVE ANALYSIS OF CYBERCRIMES IN RUSSIA AND FOREIGN COUNTRIES

V. Zudaeva
E. Kopylova
L. Erbaeva

Summary. The problem of cybercrime is distinguished by its globality and worries the entire world community. This article discusses the essence of crimes related to the field of computer technology, their main causes and possible ways to combat them. A comparative analysis of the growth dynamics of cybercrime in the Russian Federation and some foreign countries is also provided. The measures taken by various states, the fight against cybercriminals, as well as their regulatory and legal regulation are considered.

Keywords: cybercrime, legislation, threats, computer information, copyright, criminal liability, computer technology, information, hackers, cybercriminals.

Зудаева Вероника Вячеславовна
Старший преподаватель,
Восточно-Сибирский институт МВД России
veronikaz2007@mail.ru
Копылова Екатерина Евгеньевна
Восточно-Сибирский институт МВД России
katerina.kopylova.79@mail.ru
Ербаева Лариса Лазаревна
Старший преподаватель, Иркутский национальный исследовательский технический университет
lora711@mail.ru

Аннотация. Проблема киберпреступности отличается своей глобальностью и беспокоит все мировое сообщество. В данной статье рассматривается сущность преступлений, связанных со сферой компьютерных технологий, их основные причины и возможные способы борьбы с ними. Также приведен сравнительный анализ динамики роста киберпреступлений в Российской Федерации и некоторых зарубежных странах. Рассмотрены меры, принимаемые различными государствами, борьбы с киберпреступниками, а также их нормативно-правовая регламентация.

Ключевые слова: киберпреступления, законодательство, угрозы, компьютерная информация, авторское право, уголовная ответственность, компьютерные технологии, информация, сведения, хакеры, киберпреступники.

XXI век характеризуется повсеместным внедрением во все сферы жизни общества и человека достижений науки, различных компьютерных технологий и общей цифровизацией и компьютеризацией нашей страны. В связи с этим отмечается и рост преступлений в данной сфере. Развитие информационных отношений упрощает людям жизнь, делает возможным виртуальное получение, хранение, обработку важной для человека информации, также упрощает его взаимодействие с различными организациями, общение с другими людьми, ведение бизнеса и прочее, однако тем самым делает его более уязвимым перед киберпреступниками [1].

К сожалению, статистические показатели по преступлениям в сфере компьютерных технологий растут ежегодно. Так, за 2021 год в статистическую отчетность вошли 518 тысяч киберпреступлений. Эти данные превзошли показатели на 1,4 % — 2020 год и на 1,8 % — 2019 год, что и свидетельствует о стабильном росте показателя преступлений в данной сфере. Негативным фактором данного явления является и наносимый урон экономике государства. По подсчетам экспертов, деятельность киберпреступников наносит ущерб государству в размере 150 миллиардов рублей (данный показатель был рассчитан за 2021 год). Конечно же, наше государство постоянно модернизирует методы борьбы с хакерами, кибермошенниками. Министерство внутренних дел Российской Федерации постоянно взаимодействует с органами и организациями, сфера деятельности которых связана с цифровым пространством или телекоммуникациями, для повышения эффективности борьбы с данной проблемой и совершенствованию превентивных мер. Вдобавок к этому происходит и взаимодействие с другими государствами для обмена опыта в борьбе с данной проблемой, предложений по совершенствованию комплекса профилактических мероприятий, способов выявления, пресечения и привлечения к ответственности, посредством Международных конгрессов по кибербезопасности [2].

Современный этап требует совершенствования деятельности правоохранительных органов в области киберпространства, так как всем известно, что преступный мир развивается стремительнее, а особенно мир киберпреступности в связи с повсеместной цифровизацией [3]. Все государства, принимающие участие в упомянутых конгрессах, сходятся во мнении о существовании острой необходимости в сотрудничестве между государствами в сфере IT-технологий, увеличении числа высококвалифицированных специалистов в данной области в составе государственных органов по борьбе

с киберпреступностью и налаживание быстрой межгосударственной коммуникации по вопросам обмена информации о наличии киберугроз. Несомненно, проблема увеличения числа преступлений в сфере компьютерной информации существует в каждом государстве. И каждое государство борется с ней [4].

Так, в России за такой вид преступления предусмотрена уголовная ответственность (глава 28 УК РФ «Преступления в сфере компьютерной информации»). В Германии также существует запрещающая норма, прописанная в уголовном кодексе (статья 202, Daten — термин, указывающий на причастность события к киберпреступлениям). В этой Федеративной Республики с данной проблемой борются комплексно и на государственном уровне — обеспечивается общая цифровая среда, безопасность государства в информационном пространстве и безопасность экономики страны. Ну и конечно же, Германия ведет активное участие в деятельности по сотрудничеству с другими странами для объединения сил и средств в борьбе с данной проблемой.

Такая развитая во всех сферах страна, как Швейцария, также предусматривает уголовную ответственность за киберпреступления (она не прописана в отдельной главе Уголовного кодекса, однако имеется в ряде статей). Однако кибербезопасность этой страны на высоком уровне благодаря комплексному подходу в выявлении таких нарушений закона и привлечения в последствии к уголовной ответственности, которая отличается своей суровостью. Вдобавок постоянно создаются компании, например, «Kudeski», «Oneconsult», «Infoguard», которые свою деятельность направляют на снижение кибератак и др.

Данная проблема затронула даже регионы Африки. Самый яркий пример — Кения. Там преступления имеют экономический характер в сфере IT-технологий. Например, хакеры направляют атаки типа отказ в обслуживании на порты, парализуя их работу от нескольких часов до нескольких дней, нанося огромный ущерб государству, также киберпреступники осуществляют атаки на банки, выводя оттуда огромные суммы. К сожалению, специалисты в области обнаружения данных видов нарушений закона отстают от других стран в своей результативности действий (этот факт отмечен и в нашей стране), однако мировое сообщество старается всеми силами помочь разрешить эту проблему и, например, некоторые государства осуществляют совместную операцию, которая имеет своей целью создание определенной структуры на региональном уровне, которая разрабатывает совместные планы действий и проводит правоохранительные мероприятия.

Активную борьбу с киберпреступлениями ведет и Япония. Эта страна уделяет особое внимание этой проблеме, законодательно закрепляя как можно больше запретов незаконных действий, связанных с цифровым пространством. Так, например, в Японии существует своя классификация киберпреступлений, которая отличается своей обширностью, что позволяет точно определить конкретный вид киберпреступления.

Довольно результативная борьба с преступлениями в сфере компьютерных технологий происходит в США. Там государство быстро адаптирует свое законодательство на быстроизменяющуюся обстановку в преступном мире. Вдобавок происходит постоянное ужесточение наказания за нарушения закона в данной сфере. Криминализация преступлений в этой стране отличается от многих стран — существуют как специальные нормы уголовного закона за преступные посягательства в цифровом пространстве, так ответственность предусмотрена и в общих (что схоже со способом криминализации киберпреступлений в Российской Федерации) [5].

Таким образом, следует отметить, что проблема роста преступлений в сфере компьютерных технологий охватывает все страны мирового сообщества. Некоторые из них, объединяясь, стараются разрешить эту проблему совместными усилиями. Другие же направляют все силы и средства на свою внутригосударственную борьбу с преступностью. Однако все в полной мере стараются идти в ногу с совершенствованием и развитием преступного киберсообщества, постоянно модернизируя законодательство и расширяя границы ответственности за посягательства в цифровом пространстве.

ЛИТЕРАТУРА

1. Кумышева М.К., Геляхова Л.А. К вопросу о киберпреступности в России и мире // Пробелы в российском законодательстве. 2018. №4. — [Электронный ресурс]. — Режим доступа: https://searchinform.ru/survey/global-2020/ (дата обращения 04.05.2023).
2. Матчанов А. Об особенностях раскрытия и расследования киберпреступлений // ОИИ. — 2020. т. 1. — №. 1. — С. 155–165.
3. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. канд. юрид. наук. — Владивосток, 2005. — С. 36–40.
4. Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник ВИ МВД России. — 2020. — №3.
5. Шестак В.А., Адигамов А.И. Современное походы в законодательстве стран-членов ЕС к уголовной ответственности за преступления в киберпространстве // Образование и право. — 2020. — №8.

© Зудаева Вероника Вячеславовна (veronikaz2007@mail.ru); Копылова Екатерина Евгеньевна (katerina.kopylova.79@mail.ru);
Ербаева Лариса Лазаревна (lora711@mail.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»