УДК 343.3/7

© **Екатерина Евгеньевна Чередниченко**
кандидат юридических наук, доцент,
доцент кафедры уголовно-правовых дисциплин,
Владимирский филиал РАНХиГС,
г. Владимир
Cheredn@mail.ru

Cherednichenko Ekaterina Evgenievna
Candidate of Legal Sciences,
Associate Professor,
Associate Professor of the Department of Criminal Law Disciplines,
Vladimir Branch of the RANEPA,
Vladimir

© **Анна Евгеньевна Якимова**
студент юридического факультета,
Владимирский филиал РАНХиГС,
г. Владимир
anna.evgenevna.ya@mail.ru

Yakimova Anna Evgenievna
Student of the Faculty of Law,
Vladimir Branch of the RANEPA,
Vladimir

КИБЕРПРЕСТУПНОСТЬ – БУДУЩЕЕ РОССИЙСКОЙ ПРЕСТУПНОСТИ

Cybercrime is the future of Russian crime

Аннотация. В данной статье анализируется новый вид преступности – киберпреступность, который в последнее время становиться наиболее распространённым как в Российской Федерации, так и во всем мире. В основе статьи лежит собственное социологическое исследование – опрос населения. Авторы формулируют существующие в данной сфере проблемы и предлагают пути их решения.

Abstract. This article analyzes a new type of crime - cybercrime, which has recently become the most widespread both in the Russian Federation and throughout the world. The article is based on our own sociological research - a population survey. The authors formulate existing problems in this area and propose ways to solve them.

Ключевые слова: киберпреступность, компьютерная информация, уголовная ответственность.

Keywords: cybercrime, computer information, criminal liability.

Одними из наиболее распространённых преступлений в последнее время становятся киберпреступления, а киберпреступность постепенно вытесняет другие традиционные для Российской Федерации виды преступности.

По данным официальной статистики, представленной МВД РФ, за период с января по декабрь 2023 года было зарегистрировано 677,0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5 %

в январе - декабре 2022 года до 34,8 %. Более чем три четверти (77,8 %) этих преступлений совершается с использованием сети «Интернет» (526,8 тыс.; +38,2 %), почти половина (44,7 %) – средств мобильной связи (302,9 тыс.; +42,2 %) [4]. Для сравнения: в 2014 году число таких преступлений составляло лишь 10 000, т.е. за 10 лет их число выросло в 67 раз. Каждый год совершаются все более сложные кибератаки, самыми распространёнными среди которых являются:

- неправомерный доступ к компьютерной информации;
- создание вредоносных программ, фишинг;
- кража личных данных;
- мошенничество с цифровой валютой, криптоджекинг, майнинг криптовалют и т.д.

Киберпреступность представляет серьезную угрозу для государства, включая критическую инфраструктуру, военные системы и информационное пространство страны. Масштабы киберпреступности достигли таких размеров, что позволяют называть их угрозой национальной безопасности, это признал представитель Генпрокуратуры Андрей Некрасов. При этом раскрывается не более 25 % из таких преступлений, отметил он [3].

Все это требует постоянного обновления и совершенствования правовых моделей для борьбы с этим явлением.

Развитие информационных технологий и расширение цифровой инфраструктуры открывают новые перспективы для совершения киберпреступлений. Одновременно с этим прогресс в области искусственного интеллекта предоставляет возможности для более эффективной борьбы с киберугрозами. Поэтому важно исследовать, как уголовно-правовые модели могут адаптироваться к эволюции информационного пространства и использовать новейшие технологии для предотвращения киберпреступлений.

Д. В. Пучков в своей диссертационной работе, посвященной уголовно-правовой модели защиты телекоммуникаций от преступных посягательств, пишет: «Развитие в последние десятилетия сети "Интернет" усугубляет положение в этой сфере в силу ряда объективных причин. Неконтролируемая киберактивность возрастает, выходя за границы уголовно-правовой охраны, что является глобальной мировой проблемой по причине распространения современной киберпреступности за национальные рамки» [2].

Для того чтобы продемонстрировать всю актуальность и важность выбранной проблемы и получить точные сведения, нами было проведено анкетирование населения. В опросе участвовали 76 человек, это пользователи интернета разных возрастных групп, большинство из которых, а именно 81 %, используют интернет на постоянной основе. Возраст респондентов: 14-18 лет – 14 %, 18-29 лет – 38 %, 30-45 лет – 31 %, старше 45 лет – 15 %.

Среди ответивших всего 20 % не видят для себя опасности в интернет-среде, и при этом почти каждый (86 %) сталкивался с киберпреступностью, но, к сожалению, лишь половина опрошенных знают, что это такое. Многие из респондентов (56 %) не знают об ответственности за киберпреступления и, более того, о безопасности в интернете, чаще всего узнают это из новостных

источников, 17 % – от правоохранительных органов и 36 % – от родственников или друзей. Опрошенные также считают, что на совершение таких преступлений, в одинаковом процентном соотношении (60 %), людей толкают: личные качества (агрессия, ненависть, жадность и т.д.), анонимность среды интернета и чувство безнаказанности. Ответные реакции анкетируемых, ставших жертвами киберпреступников: 35 % ничего не предпринимали, посчитав это бессмысленным; 40 % не смогли вернуть утерянные данные, средства и т.д. и лишь 23 % ответивших смогли восстановить утерянное. За помощью в подобных случаях респонденты обратились бы: 64 % – в полицию, 46 % – в Министерство внутренних дел, 27 % – в Федеральную службу безопасности (ФСБ), 14 % – в Роскомнадзор и 21 % даже не знают, куда обращаться в таком случае.

По результатам опроса можно сделать несколько выводов.

1. Почти каждый из респондентов ежедневно пользуется интернет-пространством, и большая часть считают его небезопасным, так как киберпреступники придумывают новые способы воздействия.

2. Больше половины опрошенных сталкивались с киберпреступлениями и не смогли вернуть утерянные данные или средства. Здесь можно подчеркнуть, что в большинстве своём киберпреступления совершаются с корыстной целью и носят латентный характер благодаря различным программам, что делает практически невозможным изобличение преступников.

3. Стоит сделать также акцент на осведомлённости граждан: половина опрошенных считают, что ответственности за киберпреступления нет. А раз об ответственности неизвестно, значит, это будет способствовать увеличению численности таких преступлений.

Рассматривая данную проблему, можно выделить некоторые общие проблемы и недостатки при обнаружении и пресечении киберпреступлений в России.

1. Анонимность и сложность расследования: киберпреступники часто используют сложные технические методы для совершения преступлений в Сети, благодаря которым обеспечивается латентный характер. Это затрудняет их идентификацию и привлечение к ответственности.

Киберпространство охватывает пользователей интернета и информационных технологий в самых разных территориальных локациях, что позволяет киберпреступникам совершать преступления из любой точки мира. Основное преимущество в таких преступлениях – это невозможность в большинстве случаев установления преступника либо его обнаружения и пресечения киберпреступлений своевременно. Именно этими факторами объясняется низкая раскрываемость подобных преступлений. Здесь можно сделать акцент на анонимность пользователя в Сети, которая обеспечивается также программами, установленными на компьютерном устройстве, которые позволяют осуществлять деятельность через закрытые стороны интернета, позволяющие сохранить анонимность пользователя, скрыть его местоположение и защитить передачу данных. Все эти характеристики также

снижают возможности правоохранительных органов раскрыть и расследовать такие преступления, делая это практически невозможным в некоторых случаях.

2. Недостаток специалистов и ресурсов: борьба с киберпреступностью требует наличия квалифицированных специалистов и средств для расследования и пресечения таких преступлений. В России не всегда хватает квалифицированных специалистов и современного оборудования для эффективной борьбы с киберпреступностью.

Сложным является и само расследование таких преступлений. Зачастую жертвы преступлений или вообще не обращаются за помощью в правоохранительные органы, или делают это достаточно поздно, что не позволяет собрать достаточное количество доказательств, затрудняет поиск преступников и сводит на нет все оперативные мероприятия. Многие даже не всегда понимают, что в отношении них совершено преступление, не замечают этого в силу потери незначительных сумм или оправдывая сложившуюся ситуацию компьютерным сбоем.

Также негативным обстоятельством в данном случае является сложность и длительность проведения необходимых экспертиз. Именно компьютерно-техническая экспертиза является основным и наиболее эффективным способом в расследовании преступлений. Однако в силу дороговизны и сложности данные технологии не так активно внедрены в России.

***3. Недостаток международного сотрудничества*:** киберпреступность часто имеет международный характер и эффективность борьбы с ней зависит от сотрудничества между правоохранительными органами разных стран. В России существуют проблемы с международным сотрудничеством в области киберпреступности, что затрудняет расследование и пресечение таких преступлений.

Отсутствие территориальных границ и широкие возможности для анонимности повышают вероятность противоправных действий, а при должном уровне технической и организационной подготовки преступников позволяют совершать масштабные и многократные противоправные деяния, которые сложно выявить, особенно если речь идет об организованных группах, имеющих транснациональный характер.

Очевидным становится тот факт, что Россия запаздывает с мерами оперативного реагирования на киберугрозы и предупреждения киберпреступлений.

4. Устаревшее законодательство: в России есть проблемы с адаптацией законодательства к новым видам преступлений и технологическим изменениям. Киберпреступники постоянно разрабатывают новые методы и техники для совершения преступлений, что требует постоянного обновления законодательства и уголовно-правовых моделей.

В действующем Уголовном кодексе Российской Федерации киберпреступлениям посвящена глава 28, состоящая из пяти статей, регламентирующих ответственность за различные формы общественно

опасных деяний, связанных с компьютерной информацией. Однако стоит отметить, что в данной главе отсутствуют определения основных понятий, а также не предусмотрена уголовная ответственность за целый ряд общественно опасных деяний, которые уже давно существуют на практике.

На наш взгляд, целесообразно будет внести изменения в уголовное законодательство и дополнять главу 28 УК РФ, где будут размещаться составы преступлений, непосредственно связанных с сетью «Интернет», что позволит полностью охватить регулирование киберпреступлений в российском законодательстве.

Во-первых, в Уголовном кодексе РФ необходимо дать конкретное разъяснение, что представляют собой киберпреступления. Мы предлагаем в примечании к ст. 272 УК РФ закрепить следующие определение:

«Киберпреступления — это совокупность действий, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных».

Во-вторых, также следует включить в гл. 28 УК РФ новые составы преступлений, предусматривающие уголовную ответственность за новые виды киберпреступлений, которые уже сейчас являются общественно опасными:

«Статья 272.1. ***Незаконное получение информации путём фишинга***

Получение конфиденциальной информации с помощью манипуляции или обмана пользователей с целью получения доступа к их личным данным или финансовым средствам, –

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, ограничением свободы на срок до четырех лет или лишением свободы на срок до пяти лет.

Статья 272.2. ***Кибершпионаж***

Незаконное получение, использование или передача конфиденциальной информации путем взлома или с помощью технических средств в сети «Интернет» с целью шпионажа, нарушения государственной безопасности, получения коммерческих секретов, нарушения неприкосновенности частной жизни, –

наказывается лишением свободы на срок от 3 до 8 лет.

Статья 274.1. ***Кибербуллинг***

Деяние, направленное на умышленное унижение, оскорбление, угрозы или причинение психологического вреда другому лицу в сети «Интернет», путем публикации оскорбительной или унижающей честь и достоинство информации, комментариев, изображений или видео, —

наказывается штрафом в размере от 30 000 до 300 000 рублей, исправительными работами на срок до 1 года, ограничением свободы на срок до 2 лет или лишением свободы на тот же срок».

В дополнение к этому, немаловажным аспектом являются профилактические меры по противодействию киберпреступности:

- следует проводить информационные кампании и образовательные программы для повышения осведомленности граждан о кибербезопасности и методах защиты от киберпреступлений. Начинать здесь нужно с более уязвимых категорий, такими являются: пенсионеры, подростки и лица, работающие на удалёнке (мамы в декрете, фрилансеры и др.);
- можно сделать акцент на импортозамещение. Чтобы обезопасить наше государство от киберпреступности других стран, как минимум стоит задуматься о производстве собственного технического оборудования российского производства и внедрении его в общее пользование сотрудниками различных структур и всеми гражданами. Если привлечь таких изготовителей, как «Эльбрус» и «Байкал», которые специализируются на создании технического оборудования, успешно применяемого для военного обеспечения, и дать им необходимую материальную поддержку, то можно добиться желаемого результата в данном вопросе;
- необходимо проводить обучение и повышение квалификации сотрудников правоохранительных органов в рассматриваемой сфере, так как не всегда у них есть специальные познания.

Таким образом, следует согласиться с тем, что киберпреступность – это новая форма современной преступности, число таких преступлений с каждым годом будет только расти, действенных мер, к сожалению, пока не найдено. Ограничиваться только расширением ответственности нельзя, прежде всего речь должна идти о профилактических мерах и о работе с населением в сфере его информационного просвещения.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: ред. от 23.03.2024 // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 295.
2. Пучков Д. В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: автореф. дис. … д-ра юрид. наук:00.00.00 / Денис Валентинович Пучков. – Екатеринбург, 2022. – 32 с.
3. Почему киберпреступления – угроза национальной безопасности. URL: https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti (дата обращения: 03.03.2024).
4. Состояние преступности в Российской Федерации за январь – декабрь 2023 года. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751 (дата обращения: 03.03.2024).