УДК 347.6

ВЛИЯНИЕ СОЦИАЛЬНЫХ СЕТЕЙ НА РОСТ КИБЕРПРЕСТУПНОСТИ

Давыдова А.В.[1]

Студент

4 курс, Юридический институт,

Белгородский государственный национальный исследовательский университет

Россия, Белгород

Аннотация: данная статья посвящена исследованию влияния социальных сетей на увеличение уровня киберпреступности в современном мире. Автором рассматриваются факторы, способствующие развитию преступлений в сети «Интернет», а также возможные пути снижения количества совершаемых общественно опасных деяний. Также в рамках настоящей статьи анализируются точки зрения ученых, неоднократно обращавшихся к вопросу связи информационно-телекоммуникационной сети и увеличения количества преступлений, совершаемых через сеть «Интернет».

Ключевые слова: киберпреступления, социальные сети, кибератаки, уголовное преследование, международное сотрудничество.

THE INFLUENCE OF SOCIAL MEDIA ON THE GROWTH OF CYBERCRIME

[1] ***Кислицина И.Н.*** *- Научный руководитель, старший преподаватель кафедры уголовного права и процесса, Белгородский государственный национальный исследовательский университет, Россия, Белгород*

Kislitsina I.N. *- Senior Lecturer, Department of Criminal Law and Procedure, Belgorod State National Research UniversityRussia, Belgorod*

Davydova A.V.
Student 4th year, Law Institute,
Belgorod State National Research University
Russia, Belgorod

Abstract: This article examines the impact of social media on the rise in cybercrime in the modern world. The author examines the factors contributing to the rise of online crime, as well as possible ways to reduce the incidence of socially dangerous acts. This article also analyzes the perspectives of scholars who have repeatedly addressed the issue of information and telecommunications network connectivity and the rise in crimes committed via the internet.
Keywords: cybercrime, social media, cyberattacks, criminal prosecution, international cooperation.

В настоящее время социальные сети демонстрируют стремительное развитие и интеграцию в нашу повседневную жизнь, привлекая миллионы пользователей ежедневно. Одновременно с ростом социальных сетей увеличивается и число преступлений, совершаемых с использованием цифровых ресурсов. Данный феномен породил новое явление – киберпреступность, которая представляет значительную угрозу как отдельным пользователям сети «Интернет», так и крупным корпорациям и даже государствам.

Научно-технический и цифровой прогресс в области компьютерных технологий, несомненно, только растет, а, следовательно, повышается и уровень компетентности злоумышленников, наряду с этим возрастает количество компьютерных атак, при чем, в последнее время такие атаки поражают информационные ресурсы кредитно-финансовых организаций, государственных структур и известных компаний, и фирм.

Согласно статистическим данным, в 2024 году в Российской Федерации было зарегистрировано более 600 тысяч киберпреступлений[2]. Подобные цифры свидетельствуют о действительной распространенности данных преступлений в нашей стране, особенно тревожат темпы роста кибермошенничеств и попыток взлома учетных записей пользователей, в связи с чем данная тема является актуальной для исследования.

На сегодняшний день существуют следующие виды общественно опасных деяний, для которых социальные сети служат удобной площадкой:

1.Фишинг и кража личных данных является самой распространенной группой киберпреступлений, сущность которых заключается в том, что злоумышленники рассылают фальшивые письма или размещают поддельные страницы, имитирующие, например, известные бренды или государственные учреждения, с целью получения паролей, номеров карт и иной личной информации.

Самыми популярными площадками для кражи данных стали единый портал государственных услуг, а также социальные сети «ВКонтакте», «Telegram», «WhatsApp», которые отмечают ежегодных прирост преступлений.

2. Распространение вредоносного программного обеспечения через личные сообщения или публикации с целью хищения личных данных.

3. Интернет-мошенничество. Данная разновидность киберпреступлений заключается в создании поддельных профилей для привлечения жертв на платные услуги или товары, которые фактически не предоставляются.

4. Клевета путем публикации в анонимных аккаунтах ложной информации, порочащей честь и достоинство гражданина или организации.

[2] Число киберпреступлений в России [Электронный ресурс] // URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 23.10.2025).

5. Социальные сети также широко используются как площадки для продажи товаров, ограниченных в обороте, например, оружия и наркотических средств.

Р.Б. Пхитиков в своем исследовании выделяет еще одну группу преступлений – преступления против общественной безопасности. Как отмечает ученый: «группировки экстремистской и террористической направленности все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесения вреда инфраструктурам»[3].

Согласимся с мнением ученого и отметим, что преступления против общественной безопасности являются одними из самых опасных, особенно, если подготовка к ним осуществляется посредством социальных сетей, поскольку подобное виртуальное пространство обычно обеспечивает полную анонимность преступников и государственным службам с каждым годом все сложнее раскрывать подобные преступления.

Использование социальных сетей в качестве площадок для совершения преступлений обусловлено особенностями онлайн-платформ. К таким особенностям относятся:

- широкая аудитория, состоящая из миллиардов активных пользователей, привлекает преступников возможностью быстрого охвата большого количества потенциальных жертв;

- анонимность, которая заключается в возможности пользователей скрывать личную информацию о себе посредством создания фальшивых профилей, что создает иллюзию безопасности для преступников;

- доступность, позволяющая путем выполнения минимальных требований для регистрации, присоединиться и стать пользователем онлайн-платформы.

[3] Пхитиков Р.Б. Киберпреступность в социальных сетях: причины возникновения, виды, меры предупреждения // Журнал прикладных исследований. 2022. № 9. С. 143.

- техническая простота атак и низкая квалификация большинства пользователей, которые делают социальные сети легкой добычей для хакеров.

А.П. Некрасов отмечает, что «преступления в сети Интернет характеризуются высокой латентностью и низкой раскрываемостью, в том числе из-за возможности дистанционного совершения данных преступлений. Общая раскрываемость по данной категории дел составляет в среднем 20%»[4].

Ввиду низкой раскрываемости киберпреступлений как в России, так и за рубежом, борьба с ними требует объединений усилий государства, правоохранительных органов, операторов социальных сетей, в том числе иностранных, а также простых пользователей.

На сегодняшний день в Российской Федерации разрабатывается целый комплекс мер по борьбе с киберпреступностью, который включает следующие компоненты:

- образовательные кампании по повышению компьютерной грамотности, особенно среди лиц, старше 60 лет, а также подростков, которые наиболее подвержены влиянию социальных сетей.

- ужесточение наказания за правонарушения в сети.

Так, с 1 сентября 2025 года была ужесточена ответственность в сфере информации и связи, а также увеличен срок давности привлечения к административной ответственности за подобные правонарушения[5].

- создание и расширение кадрового состава в специализированных отделов полиции для расследования преступлений, совершаемых в сети «Интернет».

---

[4] Некрасов А.П. Цифровые и информационные технологии как инструменты киберпреступности в социальных сетях и мобильных связях и меры противодействия им в контексте уголовного закона Российской Федерации // Вестник ВУиТ. 2023. № 3 (105). С. 163.

[5] Обзор: «Основные изменения в КоАП РФ в 2025 году» (КонсультантПлюс, 2025) [Электронный ресурс] // URL: https://www.consultant.ru/document/cons_doc_LAW_490308/400b8f08bfac90620f076db19bb1104f36c6e196/ (дата обращения: 22.10.2025).

- совместная работа провайдеров и властей по отслеживанию подозрительных действий в социальных сетях.

Также в 2025 году Роскомнадзор запретил звонки сразу в нескольких мессенджерах, апеллируя тем, что данные социальные сети активно используются не только мошенниками, но и лицами, развязывающими политическую и национальную нетерпимость. На наш взгляд, это весьма эффективная мера, поскольку через мессенджеры «WhatsApp» и «Telegram» с момента блокировки звонков стало реализовываться на 40% меньше преступлений, нежели в прошлые месяцы 2025 года.

Мы считаем, что особенно актуальным компонентом в борьбе с киберпреступностью является также создание автоматизированных систем мониторинга, которые позволили бы оперативно выявлять подозрительные действия и пресекать попытки атак.

В.С. Соловьев в своей работе акцентирует свое внимание на том, что «для придания системности уголовному законодательству необходимо привести к единым формулировкам диспозиции и квалифицирующие признаки статей УК РФ, предусматривающих ответственность за преступления, которые возможно совершить с использованием информационно-телекоммуникационных сетей»[6].

Согласимся с мнением автора, поскольку единая терминология и единая конструкция составов преступлений облегчат процесс правоприменения, снизят частоту появления разночтений и неясностей в понимании тех или иных норм.

По мере увеличения проникновения социальных сетей в общество угроза киберпреступлений по прогнозам ученых в IT-сфере будет возрастать. В будущем ожидаются новые формы преступлений, основанных на простоте

[6] Соловьев В.С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2016. № 1. С. 71.

и анонимности в социальных сетях и мессенджерах, ввиду чего считаем необходимым проведение постоянного мониторинга угроз.

Подводя итог представленному исследованию, можно сделать вывод о том, что социальный прогресс в сфере интернет-технологий приводит к стремительному росту числа киберпреступлений, совершаемых через социальные сети.

Увеличение количества киберпреступлений обязывает уполномоченные государственные органы и разработчиков социальных сетей решать проблему на законодательном, технологическом и образовательном уровнях. Сотрудничество общественных организаций ученых в сфере информационных технологий и государства в целом, на наш взгляд, станет ключевым моментом в построении безопасной среды для пользователей социальных сетей.

Киберпреступность является объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. Киберпреступники наносят значительный ущерб как отдельным гражданам, организациям, предприятиям, так и всей национальной экономике, и мировой экономике при минимальном для себя риске. Пока существуют программы, маскирующие реальный IP-адрес, по которому можно идентифицировать местонахождение персонального компьютера правоохранительным органам сложно найти киберпреступника. А значит, привлечь к ответственности киберпреступников оказывается весьма затруднительно. На рост преступлений в данной сфере влияет: наличие многомиллионной аудитории, анонимный характер действий злоумышленников, бесплатность и доступность.

Библиографический список

1. Некрасов, А.П. Цифровые и информационные технологии как инструменты киберпреступности в социальных сетях и мобильных связях и

меры противодействия им в контексте уголовного закона Российской Федерации // Вестник ВУиТ. 2023. № 3 (105). С. 161-170.

2. Пхитиков, Р.Б. Киберпреступность в социальных сетях: причины возникновения, виды, меры предупреждения // Журнал прикладных исследований. 2022. № 9. С. 142-145.

3. Соловьев, В.С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2016. № 1. С. 60-72.

4. Обзор: «Основные изменения в КоАП РФ в 2025 году» (КонсультантПлюс, 2025) [Электронный ресурс] // URL: https://www.consultant.ru/document/cons_doc_LAW_490308/400b8f08bfac90620f076db19bb1104f36c6e196/ (дата обращения: 22.10.2025).

5. Число киберпреступлений в России [Электронный ресурс] // URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 23.10.2025).