УДК 343
DOI: https://doi.org/10.17308/law/1995-5502/2025/2/203-207

КИБЕРПРЕСТУПЛЕНИЯ: ПОНЯТИЕ, ВИДЫ, МЕРЫ ПРОТИВОДЕЙСТВИЯ

М. Ю. Пучнина
Воронежский институт МВД России

CYBERCRIMES: CONCEPT, TYPES, COUNTERACTION MEASURES

M. Yu. Puchnina
Voronezh Institute of the Ministry of the Interior of Russia

Аннотация: рассматриваются сущность киберпреступлений, их классификация и детерминанты распространения в современных условиях. Особое внимание уделяется социально и политически мотивированным кибератакам, а также противоправному распространению недостоверной информации (фейков) и использованию ферм аккаунтов. Проанализированы ключевые меры противодействия и способы повышения эффективности превентивной деятельности. Приводится обзор научной литературы и нормативно-правовых актов, рассматривающих киберпреступность как один из наиболее актуальных вызовов цифровой эпохи.
Ключевые слова: киберпреступность, фейки, фермы аккаунтов, информационная безопасность, социальная и политическая мотивация, противодействие.

Abstract: the nature of cybercrimes, their classification and determinants of their spread in modern conditions examines. Special attention is paid to socially and politically motivated cyberattacks, as well as to the unlawful dissemination of false information (fakes) and the use of large-scale fake user accounts (account farms). Key countermeasures and strategies for enhancing the effectiveness of prevention are analyzed. The study provides an overview of scientific literature and legal acts that view cybercrime as one of the most urgent challenges of the digital age.
Key words: cybercrime, fakes, account farms, information security, social and political motivation, countermeasures.

Современное общество активно использует возможности цифровых технологий практически во всех сферах жизни. Однако бурное развитие информационного пространства создает благоприятные условия для появления новых форм противоправной деятельности. Киберпреступления приобретают всё более масштабный и опасный характер. Особенно остро стоит проблема социально и политически мотивированных кибератак, цель которых – дестабилизация общественно-политической ситуации, манипуляция общественным мнением или вмешательство в избирательный процесс[1].

Несмотря на предпринимаемые меры противодействия, эффективность существующих правовых и технических инструментов нередко оказывается недостаточной, а быстрое развитие технологий усложняет задачу правоохранительных органов. Необходим систематический подход, позволяющий учитывать не только технические, но и социальные аспекты кибербезопасности. В рамках данного исследования ставится задача всесторонне проанализировать сущность и виды киберпреступлений, определяющих тенденции их популяризации, а также выявить перспективные направления совершенствования контрмер.

Анализ существующих исследований показывает, что проблема киберпреступлений широко освещается в работах российских и зару-

[1] См.: *Таков А. З.* Социальные и политические мотивированные формы проявления киберпреступности // Пробелы в российском законодательстве. 2022. № 5 С. 190–194.

бежных ученых. В частности, С. Бреннер[2] подчеркивает важность выработки международных соглашений, учитывающих специфику онлайн-пространства, и уделяет особое внимание правовым вызовам, связанным с трансграничным характером кибератак. М. Джонсон[3] рассматривает эволюцию киберпреступности, акцентируя влияние глобализации и расширения интернет-доступа на рост числа подобных правонарушений.

В российской правовой науке исследование киберпреступлений активно ведется в контексте разработки нормативных актов, а также совершенствования методов правоохранительной деятельности. Так, ряд авторов[4] классифицирует киберпреступления и дает обширный анализ правовых основ, а другие[5] подробно рассматривают специфику противодействия кибератакам, начиная от уголовно-правовых мер и заканчивая международно-правовым сотрудничеством. При этом на первый план выходит необходимость комплексного подхода: ученые сходятся во мнении, что без слаженной работы государства, коммерческих структур и общественных институтов полностью нейтрализовать угрозу киберпреступности невозможно.

В научных исследованиях и нормативно-правовой практике отсутствует единое, закрепленное на международном уровне определение «киберпреступления», однако, опираясь на положения Будапештской Конвенции Совета Европы[6] и труды ряда ученых, под киберпреступлением понимают противоправное деяние, совершаемое с использованием компьютерных систем или сетей, наносящее ущерб правам и интересам личности, общества или государства. Несмотря на то что термин «киберпреступление» используется уже продолжительное время, на сегодняшний день не существует исчерпывающего перечня действий, относящихся к данной категории. Это связано с тем, что виртуальное пространство сети Интернет постоянно претерпевает видоизменения, порождая новые формы противоправной деятельности.

Согласно УК РФ ответственность за преступления в сфере компьютерной информации наступает, если затрагиваются общественные отношения по защите информации, финансовые интересы граждан и организаций, а также иные значимые сферы. При этом Федеральный закон «Об информации, информационных технологиях и о защите информации»[7] устанавливает общие принципы распространения и защиты информации, определяет правовые основы ответственности за ее незаконную обработку.

В научной литературе существует множество подходов к классификации киберпреступлений:

1. По степени социальной опасности[8]:

– преступления низкого уровня опасности (неавторизованный доступ к личным аккаунтам);

– преступления умеренного уровня опасности (мошенничество, распространение вредоносного ПО);

– преступления высокой общественной опасности (атаки на критическую инфраструктуру, политически мотивированные кибератаки).

2. По мотиву и цели[9]:

– экономически мотивированные (финансовое мошенничество, вымогательство);

– социально мотивированные (личная выгода, личная неприязнь);

– политически мотивированные (пропаганда, саботаж, подрыв институтов государственной власти).

---

[2] См.: *Brenner S.* Cybercrime and the Law : Challenges, Issues, and Outcomes. Northeastern University Press, 2012. URL: https://www.researchgate.net/ (дата обращения: 16.02.2025).

[3] См.: *Johnson M.* Cyber Crime, Security and Digital Intelligence. 2013. URL: https://www.researchgate.net/ (дата обращения: 16.02.2025).

[4] См.: *Витвицкая С. С., Витвицкий А. А., Исакова Ю. И.* Киберпреступления : понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. № 1. С. 126–136 ; *Иванова Л. В.* Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25–33.

[5] См.: *Попов Г. И.* Киберпреступления в сфере интеллектуальной собственности : новые вызовы и уголовно-правовые механизмы реагирования // Закон и право. 2024. № 5. С. 268–274 ; *Чабукиани О. А., Зорина Е. А., Солодовник В. В.* Способы противодействия киберпреступности // Социология и право. 2020. № 3. С. 84–93.

[6] См.: Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). Доступ из информ.-правовой системы «Гарант».

[7] Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[8] См.: *Brenner S.* Op. cit.

[9] См.: *Johnson M.* Op. cit.

3. По направленности воздействия[10]:

– преступления, направленные непосредственно на сети и устройства, такие как создание и распространение вирусов, использование вредоносных программ и осуществление DoS-атак;

– противоправные деяния, использующие устройства для реализации преступной деятельности, например, рассылка фишинговых писем, кибersталкинг и кража онлайн-идентичности.

Согласно Модулю, разработаному в рамках инициативы «Образование для Правосудия» (E4J), являющейся компонентом Глобальной программы по осуществлению Дохинской декларации, выделяются следующие основные виды киберпреступлений[11]:

– деяния, направленные против конфиденциальности, целостности и доступности компьютерных данных или систем;

– деяния, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда;

– деяния, связанные с содержанием компьютерных данных.

Конвенция о преступности в сфере компьютерной информации ETS № 185 подразделяет все киберпреступления на 4 категории[12]:

1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, перехват; вмешательство в данные и в систему);

2) преступления, связанные с использованием компьютера как средства совершения преступлений, т. е. как средство манипуляции информацией (компьютерное мошенничество и подлог);

3) преступления, связанные с содержанием данных, размещенных в компьютерных сетях (детская порнография);

4) преступления, связанные с нарушением авторского права и смежных прав.

В научном сообществе Будапештская Конвенция Совета Европы считается одной из наиболее строгих мер международного противодействия компьютерным преступлениям[13]. Именно по этой причине, на наш взгляд, она и не была подписана Российской Федерацией.

На основании анализа приведенных выше подходов можно предложить собственную классификацию, подчеркивающую актуальность проблемы распространения фейков и ферм аккаунтов, а также рост социально и политически мотивированных атак:

– киберпреступления, связанные с манипуляцией информацией: распространение недостоверной информации, фейковых новостей, «информационных вбросов», использование ферм аккаунтов для формирования фальшивой общественной поддержки или дискредитации конкурентов;

– киберпреступления, направленные на нарушение конфиденциальности и целостности данных: взломы, кражи персональных данных, хактивизм, кибершпионаж;

– киберпреступления против критической инфраструктуры: атаки на системы жизнеобеспечения, финансовые и государственные ресурсы, которые могут носить террористический или политический характер.

Данная классификация отражает растущую роль информационных манипуляций, применяемых в социальных сетях и мессенджерах. Особое место занимают фермы аккаунтов, позволяющие искусственно распространять фейковые сообщения и влиять на общественные настроения. Важно отметить, что борьба с киберпреступностью требует не только постоянного совершенствования правовых норм, но и внедрения современных технологий для предотвращения и расследования таких преступлений.

Важным аспектом современного понимания киберпреступности становится активное распространение социально и политически мотивированных атак. Как уже было отмечено ранее, их цель не только получение финансовой выгоды, но и воздействие на общественное сознание, дестабилизация общественных институтов, совершение актов информационного террора или пропаганды. Кибератаки на критическую инфраструктуру, взлом правительственных порта-

[10] См.: *Миронов Б. А., Милаева М. Ю.* Современный взгляд на понятие преступления в сфере компьютерной информации // Скиф. Вопросы студенческой науки. 2024. № 10(98). С. 248–254.

[11] Киберпреступность 2. Основные виды киберпреступности. Образование во имя правосудия. Серия университетских модулей Киберпреступность / ООН, Вена. 2019. URL: https://www.unodc.org/documents/e4j/Cybercrime/ Cybercrime_Module_2_General_Types_of_Cybercrime_RU.pdf (дата обращения: 16.02.2025).

[12] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). Доступ из информ.-правовой системы «Гарант».

[13] См.: *Простосердов М. А.* Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. … канд. юрид. наук. М., 2016. 232 с.

лов, манипуляция результатами выборов и распространение фейков – всё это разновидности политически опасных киберпреступлений, которые требуют применения специальных мер противодействия.

В современных условиях особую актуальность приобретают такие виды киберпреступлений, как распространение ложной информации (фейков) и использование так называемых фермерских аккаунтов – больших массивов недостоверных учетных записей. Ложная информация, появляясь в интернете, моментально распространяется среди пользователей, вызывая бурную общественную реакцию. Стоит подчеркнуть, что возрастная группа аудитории здесь не играет существенной роли: пожилые люди из-за ограниченного доступа к альтернативным источникам информации, а молодежь вследствие недостаточной критической оценки воспринимают подобные сведения как достоверные. Такой подход к потреблению информации способствует формированию цепной реакции: сначала пользователи попадают под влияние панических настроений, затем начинают активно транслировать их дальше.

Взаимосвязь между распространением фейковых новостей и деятельностью ферм аккаунтов заслуживает более детального анализа. Администраторы таких ферм создают иллюзорный слой общественного мнения, выражающий заранее сформулированные взгляды, что значительно усиливает воздействие ложной информации на реальных пользователей. Этот феномен можно проиллюстрировать на примере политических новостей, сопровождающихся значительным количеством негативных комментариев. Индивид, изучая подобные мнения, зачастую подвергается их воздействию, что может привести к искаженному восприятию происходящего и даже вовлечению в противоправные действия.

Противодействие киберпреступлениям социального и политического характера требует внедрения стратегий, базирующихся на распространении позитивного контента. Принцип «клин клином» находит здесь практическое применение: позитивная информация, распространяемая при поддержке инфлюэнсеров, может эффективно контрастировать с негативным потоком и способствовать формированию конструктивных общественных настроений. Это особенно важно в контексте популяризации идей и ценностей, значимых для общества и государства.

Для минимизации рисков, связанных с киберпреступностью, необходимо реализовать следующие меры: повышение общего уровня исторической и информационной грамотности среди населения; адаптация и модернизация законодательства с учетом новых вызовов; развитие IT-индустрии и технологического сектора; привлечение блогеров и лидеров общественного мнения к профилактическим мероприятиям; увеличение объемов позитивного социального контента в интернет-пространстве. Указанные направления представляют собой комплексный подход к решению проблемы, что позволяет не только реагировать на возникающие угрозы, но и эффективно их предупреждать.

Библиографический список

Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления : понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. № 1. С. 126–136.

Иванова Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25–33.

Миронов Б. А., Милаева М. Ю. Современный взгляд на понятие преступления в сфере компьютерной информации // Скиф. Вопросы студенческой науки. 2024. № 10(98). С. 248–254.

Попов Г. И. Киберпреступления в сфере интеллектуальной собственности : новые вызовы и уголовно-правовые механизмы реагирования // Закон и право. 2024. № 5. С. 268–274.

Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. … канд. юрид. наук. М., 2016. 232 с.

Таков А. З. Социальные и политические мотивированные формы проявления киберпреступности // Пробелы в российском законодательстве. 2022. № 5 С. 190–194.

Чабукиани О. А., Зорина Е. А., Солодовник В. В. Способы противодействия киберпреступности // Социология и право. 2020. № 3. С. 84–93.

Brenner S. Cybercrime and the Law : Challenges, Issues, and Outcomes. Northeastern University Press, 2012. URL: https://www.researchgate.net/

Johnson M. Cyber Crime, Security and Digital Intelligence. 2013. URL: https://www.researchgate.net/

References

Vitvitskaya S. S., Vitvitsky A. A., Isakova Yu. I. Cybercrimes : concept, classification, international counteraction // Legal order and legal values. 2023. No. 1. P. 126–136.

Ivanova L. V. Types of cybercrimes under Russian criminal law // Legal research. 2019. No. 1. P. 25–33.

Mironov B. A., Milaeva M. Y. Modern view on the concept of crime in the field of computer information // The Skiff. Questions of student science. 2024. No. 10(98). P. 248–254.

Popov G. I. Cybercrimes in the field of intellectual property : new challenges and criminal law response mechanisms // Law and order. 2024. No. 5. P. 268–274.

Prostoserdov M. A. Economic crimes committed in cyberspace and measures to counter them : cand. legal sci. dis. Moscow, 2016. 232 p.

Takov A. Z. Social and politically motivated forms of manifestation of cybercrime // Gaps in Russian legislation. 2022. No. 5. P. 190–194.

Brenner S. Cybercrime and the Law : Challenges, Issues, and Outcomes. Northeastern University Press, 2012. URL: https://www.researchgate.net/

Johnson M. Cyber Crime, Security and Digital Intelligence. 2013. URL: https://www.researchgate.net/

Воронежский институт МВД России.

Пучнина М. Ю., кандидат юридических наук, старший преподаватель кафедры уголовного права и криминологии

E-mail: masloy100@mail.ru

Поступила в редакцию: 17.02.2025

Для цитирования:

Пучнина М. Ю. Киберпреступления: понятие, виды, меры противодействия // Вестник Воронежского государственного университета. Серия: Право. 2025. № 2 (61). С. 203–207. DOI: https://doi.org/10.17308/law/1995-5502/2025/2/203-207

Voronezh Institute of the Ministry of the Interior of Russia.

Puchnina M. Yu., Candidate of Legal Sciences, Senior Lecturer of the Department of Criminal Law and Criminology

E-mail: masloy100@mail.ru

Received: 03.02.2024

For citation:

Puchnina M. Yu. Cybercrimes: concept, types, counteraction measures // Proceedings of Voronezh State University. Series: Law. 2025. No 2 (61). P. 203–207. DOI: https://doi.org/10.17308/law/1995-5502/2025/2/203-207