

УДК 343.

ГРНТИ 10.81

EDN: WFESTI



## 4.14. Об актуальных проблемах противодействия киберпреступлениям в условиях цифровой трансформации

©Карчаева Камила Аварьевна  
Северо-Кавказский институт повышения квалификации (филиал)  
Краснодарского университета МВД России, г.Нальчик, КБР, Россия  
kamila.karchayeva@mail.ru

**Аннотация:** Актуальность выбранной темы научного исследования объясняется тем, что в условиях нарастающей агрессии зарубежных стран информационные ресурсы и защита от «информационных атак» является приоритетной задачей государства. Цифровая трансформация представляет собой объединение всего мирового сообщества в единое информационное поле, что, безусловно, положительно влияет на процессы жизнедеятельности людей, упрощая возможность получения услуг, доступа к информации, проведение международных операций и осуществления сотрудничества. Однако масштабное развитие сети «Интернет» помимо прогрессивных проявлений несет новые угрозы и вызовы, создавая условия для совершения преступлений против отдельных граждан, организаций или государств.

Целью исследовательской работы является анализ основных видов киберпреступлений, а также проблем, связанных с противодействием данным видам административных правонарушений и преступлений.

Автор приходит к выводу о том, что киберпреступность – это угроза безопасности всего мирового сообщества. За счет широкого охвата аудитории в сети, сложности расследования такого рода преступлений, высокой конфиденциальности и неумения ориентироваться в особенностях современного кризисного информационно-коммуникационного взаимодействия наблюдается ежегодный рост киберпреступлений по всему миру.

**Ключевые слова:** киберпреступления, средства массовой информации, сеть «Интернет», противодействие преступлениям в адрес России, преступления в сети «Интернет», фейки, защита информации, кибератака, киберпреступник.

**Для цитирования:** Карчаева К.А. Об актуальных проблемах противодействия киберпреступлениям в условиях цифровой трансформации // Пробелы в российском законодательстве. 2023. Т. 16. №4. С. 336-340. EDN: WFESTI

## Current Problems of Countering Cybercrime in the Context of Digital Transformation

©Karchaeva Kamila Avarievna  
North Caucasus Institute for Advanced Studies (branch)  
of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia  
kamila.karchayeva@mail.ru

**Abstract:** The relevance of the selected topic of scientific research is explained by the fact that in the context of the increasing aggression of foreign countries, information resources and protection against "information attacks" is a priority for the state. Digital transformation is the unification of the entire world community into a single information field, which, of course, has a positive effect on people's life processes, simplifying the possibility of obtaining services, access to information, conducting international operations and implementing cooperation. However, the extensive development of the Internet, in addition to progressive manifestations, brings new threats and challenges, creating conditions for the commission of crimes against individuals, organizations or States.

The purpose of the research is to analyze the main types of cybercrime, as well as the problems related to countering these types of administrative offenses and crimes.

The author concludes that cybercrime is a threat to the security of the entire world community. By reaching a wide audience online, the complexities of investigating such crimes, the high level of confidentiality and the inability to

*navigate in the features of the modern crisis information and communication interaction, there is an annual increase in cybercrime around the world.*

**Keywords:** *cybercrime, mass media, Internet, countering crimes against Russia, crimes on the Internet, fakes, information protection, cyberattack, cybercriminal.*

**For citation:** *Karchaeva K.A. Current Problems of Countering Cybercrime in the Context of Digital Transformation // Gaps in Russian Legislation. 2023. Vol. 16. №4. Pp. 336-340. (in Russ.). EDN: WFESTI*

## ВВЕДЕНИЕ

Глобализация представляет собой процесс всеобщей интеграции, при котором все мировое сообщество выступает как единое информационное поле.

Действительность сложно представить без доступа к сети «Интернет», посредством которой организован доступ практически ко всем государственным услугам, торговым площадкам и базам данных. Помимо положительного эффекта от широкого применения современных информационно-технических средств повсеместное использование ресурсов сети «Интернет» несет и угрозы, такие как распространение недостоверной информации, клеветы, кража личных данных пользователей и финансовых активов с банковских карт. Самыми распространенными видами киберпреступлений являются кибершантаж, кибершпионаж, осуществление мошеннических операций. Широкое использование ресурсов «Интернет», а также современных информационно-технических средств обусловило рост информационных преступлений во всем мировом сообществе.

Преступление, совершенное в сети «Интернет» - это преступление совершенное при помощи современных информационно-технических средств и ресурсов сети «Интернет».

История киберпреступности берет свое начало с появления первых ЭВМ и условно состоит из двух периодов, первый - с момента создания первой ЭВМ до 1990 года и современный период - с 1990 года по настоящий момент времени. Следует отметить, что сейчас киберпреступность набирает обороты и несет угрозу национальным интересам Российской Федерации и всего мирового сообщества.

Угроза Интернет-преступлений объясняется высоким уровнем конфиденциальности такого характера преступлений, широким охватом аудитории в сети, цифровой и правовой неграмотностью населения, сложностью поиска преступников в сети и блокирования сайтов и страниц мошенников, а также неумением ориентироваться в особенностях современного кризисного информационно-коммуникационного взаимодействия.

Анализу актуальных проблем противодействия киберпреступлениям уделяли внимание многие авторы и ученые, среди которых отметим труды З.Л. Шагапсова, Л.А. Буряевой, Е.А. Алиевой, Е.Р. Николаевой, А.П. Суходолова, Р.Г.Кочоян, М.К.Кумышевой.

Однако, несмотря на достаточно глубокий анализ выбранной темы научного исследования научными деятелями и учеными, мы наблюдаем рост преступлений в сети «Интернет», а также возрастание агрессии к Российской Федерации со стороны мирового сообще-

ства, что делает проблему защиты национальных информационных ресурсов еще более актуальной.

## ВИДЫ ПРОТИВОПРАВНЫХ ДЕЯНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Среди комплекса определений термина «киберпреступление» выделим и проанализируем следующие. Д.Н. Карповой киберпреступность определена как социальная девиация, осуществляемая посредством технических средств с доступом в сеть «Интернет», цель которой нанесение культурного, идеологического, экономического и других видов ущерба отдельному гражданину, организации или государству [6].

Также можно определить киберпреступность как любую противоправную деятельность, осуществляемую в виртуальном пространстве при помощи современных информационно-технических средств и технологий.

М. Е. Батухтин в своих научных работах определяет киберпреступление как преступную деятельность в электронной системе, осуществляемая посредством компьютерных средств либо против них [5].

Рост преступлений в сети «Интернет», а также посредством современных информационно-технических средств усугублен также внешнеполитической обстановкой, характеризующейся нестабильностью и угрозами, связанными с активной деятельностью запрещенной в России организацией «ИГИЛ», которая посредством различных информационных платформ осуществляет вербовку молодежи в ряды запрещенных вооруженных формирований, с активизацией незаконного оборота наркотических средств и психотропных веществ, а также экономических санкциями против РФ и ситуацией на Украине.

Прежде чем рассмотреть основные проблемные аспекты противодействия киберпреступлениям, выделим и рассмотрим основные виды преступлений в сети.

В самом широком смысле все киберпреступления можно разделить на две группы: насильственные и ненасильственные.

Среди насильственных основными являются: угроза физической расправы, киберпреследования, киберэкстремизм и кибертерроризм. К ненасильственным относятся: кибермошенничество, кибершантаж, киберворовство, незаконный оборот наркотических средств и психотропных веществ, азартные игры в сети «Интернет», отмывание денег с помощью электронного перемещения.

Свободный доступ к информационному полю усугубил и усложнил процесс расследования и противодействия преступлениям, связанным с распростране-

нием наркотических средств и психотропных веществ, а также деструктивной религиозной и политической идеологии. Данные виды противоправных деяний широко распространены в рядах молодежи, что имеет особенно негативное влияние на национальные интересы общества.

### **ОСНОВНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ**

Защита информации – это деятельность, направленная на охрану данных от несанкционированного доступа и атак злоумышленников.

На современном этапе развития общества правоохранительная система сталкивается с рядом проблем, основными из которых являются высокая конфиденциальность совершения киберпреступлений, широта охвата аудитории в сети, высокая степень искажения реальных фактов и информации, недостаточная правовая и цифровая грамотность населения.

Основными видами защиты информации являются следующие:

- физическая защита, которая представляет собой обеспечение физических барьеров на пути к охраняемой информации;
- правовая защита, регламентирующая использование качественного нормативно-правового обеспечения;
- техническая защита предполагает защиту информационных ресурсов некриптографическими методами;
- криптографическая защита информации представляет защиту информации при помощи криптографического преобразования.

Целью защиты информации от атак киберпреступников является сокращение негативного влияния на информационное поле и сведение к минимуму информационных потерь.

Основными задачами кибербезопасности являются:

- совершенствование нормативно-правовой и законодательной базы в области обеспечения кибербезопасности;
- своевременное пресечение угроз со стороны киберпреступников;
- минимизация ущерба от атак мошенников на информационную среду;
- пресечение посягательств на информационные ресурсы и персонал на основе нормативно-правовых механизмов.

Данные задачи должны быть решены на основе принципов законности, непрерывного мониторинга угроз со стороны злоумышленников, применения современных технических средств и криптографических методов защиты информации, а также приоритета национальных интересов в области защиты критической информационной инфраструктуры.

Отметим особенности преступлений, совершаемых с использованием современных информационно-технических средств и ресурсов сети «Интернет».

Во-первых, высокий уровень конфиденциальности данного вида преступлений, что усложняет идентификацию преступника.

Во-вторых, международный характер киберпреступлений, что связано с процессами глобализации, объ-

единяющими все мировое общество в единое информационное поле.

В-третьих, интернет-преступность нацелена на широкую сетевую аудиторию, причём довольно различным по поло-возрастным, социальным и национальным характеристикам.

В-четвертых, многоэпизодный характер преступных действий при множественности потерпевших;

В – пятых, зачастую продолжительный временный диапазон между временем совершения преступления и наступлением его последствий, а также неосведомленность потерпевших о том, что они подверглись преступному воздействию;

В-шестых, необходимость современных технических средств, нормативно-правовых рычагов и знаний компетентных лиц в направлении блокирования киберпреступлений.

Проводя анализ статистических данных и мирового опыта борьбы с киберпреступностью, следует отметить, что уровень преступлений в Интернет-пространстве России на сегодняшний день относится к категории высоких. Что обусловлено следующими предпосылками:

- слабая правовая регламентация процессов использования информационных ресурсов и несовершенство законодательства в области киберпреступности;
- сложность расследования киберпреступлений и идентификации личности преступника;
- динамика развития киберпространства, развитие новых методик проведения кибератак, а также появление новых форм и видов противоправных деяний, с использованием данных информационных площадок;
- отсутствием общей методики борьбы с киберпреступлениями.

Ввиду вышесказанного необходимо разработать методику противодействия угрозам со стороны киберпреступников, что позволит осуществить защиту информационно-цифрового суверенитета государства и отдельных граждан от различных атак противников.

Для предотвращения и нейтрализации последствий применения информационного оружия рекомендуется принять следующие меры:

- обеспечение физической защиты информации и ее носителей;
- защита информационной составляющей при помощи технических средств, то есть посредством некриптографических механизмов;
- обеспечение контроля за стабильной и бесперебойной работой банков данных;
- минимизация ущерба от несанкционированного доступа противника к информационным ресурсам;
- осуществление охраны национальных информационных ресурсов и их конфиденциальная передача по открытым информационным площадкам и сетям;
- непрерывный мониторинг за объектами критической информационной инфраструктуры государства;
- использование качественного программного обеспечения и лицензионных технических средств;
- использование сильных и сложных паролей;
- запрет на переход по ссылкам и сообщениям подозрительного содержания;
- осуществление минимального количества идентичных процедур.

## ВЫВОДЫ

Кибератака – это несанкционированная и осуществляемая сознательно попытка преступника проникнуть в информационное поле другого человека или организации с определенной целью, например, кража данных, взлом компьютера и так далее.

Киберпреступность на сегодняшний день одна из главных угроз национальным интересам России и всего мирового сообщества. Тем самым противодействие атакам злоумышленников является приоритетной задачей правоохранительной системы. Проведя анализ всех проблем, нами разработаны основные механизмы противодействия преступлениям, совершаемым с использованием сети «Интернет», в сложившихся правовых реалиях с учетом следующих особенностей:

1. Повсеместное развитие сети «Интернет» позволяет сделать вывод, что продолжится рост преступности посредством применения современных информационно-технических средств. Таким образом, видится необходимым повышение правовой и цифровой грамотности населения.

2. Профилактическая работа с отдельными категориями пользователей сети «Интернет», например, молодежью, как лицами представляющими интерес для правоохранительной системы, так как указанная возрастная категория населения ввиду современных технических знаний и навыков являются потенциально опасными в указанной сфере.

3. Повсеместное введение и обеспечение обязательной и достаточной идентификации личности пользо-

вателя при предоставлении доступа в сети Интернет в местах коллективного пользования. [11]

4. Обобщение судебной и следственной практики по пресечению киберпреступлений, а также разработка единой методики расследования преступлений, совершаемых с использованием современных информационно-технических средств.

5. Обмен опытом между государствами и международное сотрудничество в направлении блокирования деятельности киберпреступников.

## ЗАКЛЮЧЕНИЕ

Как показывает практика, преступления, осуществляемые в сети «Интернет» или при помощи современных информационно-технических средств, широко распространяются и несут угрозу всему мировому сообществу.

Противодействовать им позволяет лишь применение широкого спектра физических, технических, правовых и криптографических методов.

Представляется целесообразным постоянное сотрудничество и обмен опытом между государствами в направлении блокирования сайтов и страниц преступников, а также разработки единого механизма противодействия преступлениям в сети «Интернет».

Сотрудники правоохранительной сферы постоянно должны повышать квалификацию, уровень профессиональных компетенций и специальных технических знаний в направлении противодействия и профилактики киберпреступности в условиях современных правовых реалий.

ЛИТЕРАТУРА

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
2. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.02.2021).
3. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 30.12.2020).
4. Алиева Е.А. Сеть интернет как средство совершения развратных действий // Пробелы в российском законодательстве. 2017. № 4. С. 180-182.
5. Батухтин М. Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. 2018.
6. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. Том. 22. № 8. С. 46-50.
7. Кочоян Р.Г. Противодействие преступлениям, совершаемым в сети «Интернет»: совершенствование уголовного законодательства Российской Федерации // Криминальные реалии, реагирование на них и закон / под редакцией А.И. Долговой. Москва, 2018. С. 127-131.
8. Кумышева М.К. Проблемы противодействия интернет-преступности в Российской Федерации // Проблемы экономики и юридической практики. 2019. № 3. С. 97-98.

REFERENCES

1. Federal Law "On information, information technologies and information protection" dated July 27, 2006 N 149-FZ (last edition).
2. "Code of the Russian Federation on Administrative Offenses" dated December 30, 2001 N 195-FZ (as amended on February 4, 2021).
3. "Criminal Code of the Russian Federation" dated 06/13/1996 N 63-FZ (as amended on 12/30/2020).
4. Alieva E.A. The Internet as a means of committing indecent acts // Gaps in Russian legislation. 2017. No. 4. P. 180-182.
5. Batukhtin M. E. Cybercrimes: causes, types, forms, consequences, directions of counteraction // Problems and prospects for the development of the penitentiary system of Russia at the present stage Proceedings of the International Scientific Conference of adjuncts, graduate students, cadets and students. 2018.
6. Karpova D.N. Cybercrime: a global problem and its solution // Power. 2014. Vol. 22. No. 8. P. 46-50.
7. Kochoyan R.G. Counteraction to crimes committed on the Internet: improvement of the criminal legislation of the Russian Federation // Criminal realities, response to them and the law / edited by A.I. Debt. Moscow, 2018, pp. 127-131.
8. Kumysheva M.K. Problems of combating Internet crime in the Russian Federation // Problems of Economics and Legal Practice. 2019. No. 3. P. 97-98.

9. Николаева Е.Р. Проблемы противодействия преступлениям, совершаемым в сети Интернет // Вопросы российской юстиции. 2019. № 4. С. 417-424.
10. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 1 (24) 2012.
11. Суходолов А.П., Иванцов С.В., Борисов С.В., Спасенников Б.А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей. // Байкальский государственный университет, г. Иркутск, Российская Федерация. Всероссийский криминологический журнал. 2017. Т. 11, № 1. С. 13–21; <https://cyberleninka.ru/article/n/aktualnye-problemy-preduprezhdeniya-prestupleniy-v-sfere-ekonomiki-sovershaemyh-s-ispolzovaniem-informatsionno>
12. Урбан В.В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестник Восточно-сибирского института МВД России. 2019. № 1 (88). С. 55-63.
13. характеристика состояния преступности в Российской Федерации за январь-февраль 2021 года. <https://мвд.рф/reports/item/23447482/>.
9. Nikolaeva E.R. Problems of countering crimes committed on the Internet // Issues of Russian justice. 2019. No. 4. P. 417-424.
10. Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat // Criminology: yesterday, today, tomorrow. 1 (24) 2012.
11. Sukhodolov A.P., Ivantsov S.V., Borisov S.V., Spasennikov B.A. Actual problems of preventing crimes in the sphere of the economy committed using information and telecommunication networks. // Baikal State University, Irkutsk, Russian Federation. All-Russian criminological journal. 2017. V. 11, No. 1. P. 13–21; <https://cyberleninka.ru/article/n/aktualnye-problemy-preduprezhdeniya-prestupleniy-v-sfere-ekonomiki-sovershaemyh-s-ispolzovaniem-informatsionno>
12. Urban V.V. Crimes committed using information and telecommunication networks: general characteristics and criminal procedural measures to counter them // Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. No. 1 (88). pp. 55-63.
13. characteristics of the state of crime in the Russian Federation for January-February 2021. <https://mvd.rf/reports/item/23447482/>.

#### РЕЦЕНЗИЯ

на статью старшего преподавателя кафедры организации правоохранительной деятельности СКИ(ф) КрУ МВД России Карчаевой К.А. на тему «Об актуальных проблемах противодействия киберпреступлениям в условиях цифровой трансформации»

Киберпреступность на сегодняшний день одна из главных угроз национальным интересам России и всего мирового сообщества. Тем самым противодействие атакам злоумышленников является приоритетной задачей правоохранительной системы.

На современном этапе развития общества правоохранительная система сталкивается с рядом проблем, основными из которых являются высокая конфиденциальность совершения киберпреступлений, широта охвата аудитории в сети, высокая степень искажения реальных фактов и информации, недостаточная правовая и цифровая грамотность населения.

Представленная на рецензирование работа носит научный характер. Статья хорошо структурирована, написана на четком и понятном языке, выводы логичны, литература соответствует заявленной тематике.

Цель научного исследования достигнута, автором проведён анализ основных видов киберпреступлений, а также проблем, связанных с противодействием данным видам административных правонарушений и преступлений.

В целом, статья «Об актуальных проблемах противодействия киберпреступлениям в условиях цифровой трансформации» отвечает требованиям, предъявляемым к подобного рода работам и может быть опубликована в открытой печати.

Рецензент: кандидат юридических наук, начальник кафедры организации правоохранительной деятельности СКИ(ф) КрУ МВД России, майор полиции Л.А. Геляхова

Статья прошла проверку системой «Антиплагиат»; оригинальность текста – 80,65%

Статья поступила в редакцию 22.05.2023, принята к публикации 20.06.2023

The article was received on 22.05.2023, accepted for publication 20.06.2023

#### СВЕДЕНИЯ ОБ АВТОРЕ

**Карчаева Камила Аварьевна**, канд. экон. наук, старший лейтенант полиции, старший преподаватель кафедры организации правоохранительной деятельности Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России. E-mail: [kamila.karchayeva@mail.ru](mailto:kamila.karchayeva@mail.ru)

#### ABOUT THE AUTHOR

**Karchaeva Kamila Avarievna**, Cand.Sci.(Econ.), Police Senior Lieutenant, Senior Lecturer of the Department of Law Enforcement Organization of the North Caucasus Institute of Advanced Training (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia. E-mail: [kamila.karchayeva@mail.ru](mailto:kamila.karchayeva@mail.ru)