УДК 343.148.5

С. Н. **Кольчуганок,** ***Д. А. Шитик***
Кузбасский государственный технический университет им. Т.Ф. Горбачева, Кемерово, Россия

ОСОБЕННОСТИ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В РОССИИ И ЗА РУБЕЖОМ

научный руководитель: д.ф.н., профессор кафедры истории, философии и социальных наук Золотухин В.М.

В статье рассматриваются вопросы возникновения, распространения и формы проявления киберпреступности. Выявлены как сходство, так и различия в борьбе с киберпреступностью в сфере российского и зарубежного правоприменения. Акцентировано внимание на выработку единой политики правоприменения, социально-экономических и иных механизмов в борьбе с киберпреступностью. Подчеркнуто, что специфика региональных рынков, законодательных основ и культурных особенностей может влиять на преобладание той или иной формы преступления в конкретной стране.

Ключевые слова: киберпреступность, новые технологии, социальная реальность, цифровое пространство, идентификационное мошенничество.

В современном мире, где технологии играют ключевую роль во многих аспектах нашей жизни, киберпреступность становится одной из наиболее остро стоящих проблем. Киберпреступность – это незаконные действия, совершаемые с использованием компьютерных технологий, направленные на нарушение конфиденциальности, целостности и доступности информационных ресурсов. С каждым годом количество таких преступлений растет, а их сложность увеличивается, что требует новых подходов к их предотвращению и расследованию в рамках национальных стандартов правоприменения и борьбы с киберпрступностью [Золотухин, 2018; Золотухин, 2020; Золотухин, 2021].

Россия, как и многие другие страны, сталкивается с рядом угроз в сфере кибербезопасности. Однако каждая страна разрабатывает свои методы и стратегии борьбы с этим видом преступности, опираясь на свои законодательные, технологические и культурные особенности [Золотухин, Степанцова, 2015; Степанцова, 2023]. Сравнение опыта России и зарубежных стран в этой области позволит выявить наиболее эффективные практики, а также области, требующие дополнительного внимания и усилий [Концепция, 2013].

В России первые случаи киберпреступлений были зафиксированы в 90-х годах XX века, когда начало активно развиваться интернет-пространство. Пре-

ступления, в основном, были связаны с мошенничеством, взломом и распространением вредоносного ПО. С течением времени, с увеличением числа интернет-пользователей и развитием электронной коммерции, киберпреступления стали более сложными и многочисленными [Могилевцева, Съедина, Филина, 2022; Иванова, Ильиченкова, 2023].

За рубежом ситуация развивалась аналогичным образом, однако в некоторых странах, таких как США и страны Западной Европы, проблема киберпреступности стала актуальной еще раньше из-за более раннего и активного внедрения информационных технологий. В этих странах уже в 80-х годах XX века начали формироваться первые законодательные акты, регулирующие вопросы кибербезопасности [Иванова, Съедина, 2023].

Важным этапом в истории борьбы с киберпреступностью стало осознание необходимости международного сотрудничества. Киберпреступления часто не имеют границ, и их расследование требует координации усилий разных стран. В начале 2000-х годов были приняты первые международные договоры в этой области, например, Конвенция о киберпреступности Совета Европы [Концепция, 2013]. История развития киберпреступности и борьбы с ней показывает, что это явление постоянно эволюционирует, адаптируясь к новым технологическим и социальным реалиям. Это требует постоянного мониторинга ситуации и корректировки подходов к противодействию киберугрозам как на национальном, так и на международном уровне.

Киберпреступления представляют собой широкий спектр незаконных действий, совершаемых в цифровом пространстве. В России, наиболее распространенными формами преступности являются: **фишинг** (мошеннические действия, направленные на получение конфиденциальных данных пользователей (логины, пароли, данные банковских карт) путем маскировки под доверенные источники); **DDoS-атаки** (нападения на серверы и веб-сайты с целью их временного или постоянного выведения из строя); **Распространение вредоносного ПО** (создание и распространение программ, предназначенных для незаконного доступа к информации, ее уничтожения или блокировки); **мошенничество**

в электронной коммерции (незаконные действия, связанные с мошенничеством при онлайн-покупках или продажах) [Мордвинов, Удавихина, 2022].

За рубежом к таким формам принято относить: Ransomware (вымогательское ПО) (атаки, при которых вредоносное программное обеспечение блокирует доступ к данным пользователя или организации, требуя выкуп за их разблокировку); **идентификационное мошенничество** (незаконное использование личной информации другого человека для получения материальной выгоды); **кибершпионаж** (незаконное проникновение в информационные системы с целью сбора конфиденциальной информации) и, **кибертерроризм** (использование цифровых технологий для террористических целей, например, атаки на критически важные объекты инфраструктуры) [Золотухин, Логинова, 2018: Zolotukhin, Bikmetov, Shiller, Tarasenko, 2021].

Сравнивая основные формы киберпреступлений в России и за рубежом, можно заметить, что многие из них схожи или идентичны. Однако специфика региональных рынков, законодательных основ и культурных особенностей может влиять на преобладание той или иной формы преступления в конкретной стране. Так, например, в развитых странах Запада кибертерроризм и кибершпионаж могут представлять более высокую угрозу из-за наличия критически важных объектов и большого объема конфиденциальной информации. В то время как в России проблема фишинга и DDoS-атак может быть более актуальной из-за особенностей интернет-пространства и поведения пользователей [ENISA, 2020].

Сравнивая основные формы киберпреступлений в России и за рубежом, можно заметить, что многие из них схожи или идентичны. Однако специфика региональных рынков, законодательных основ и культурных особенностей может влиять на преобладание той или иной формы преступления в конкретной стране. Так, например, в развитых странах Запада кибертерроризм и кибершпионаж могут представлять более высокую угрозу из-за наличия критически важных объектов и большого объема конфиденциальной информации. Как подчеркивает С. Бойко, «США считали, что главной угрозой являются непре-

кращающиеся нападения организованных преступных группировок, компьютерных пиратов и негосударственных субъектов, включая террористов. В то же время в отношении использования информационных технологий в военных целях американцы считали, что совершенно нет необходимости принимать какую-либо международную конвенцию» [Бойко, 2023].

В то время как в России проблема фишинга и DDoS-атак может быть более актуальной из-за особенностей интернет-пространства и поведения пользователей [ENISA, 2020]. Борьба с киберпреступностью в России включает в себя разносторонние методы, направленные на предотвращение, выявление и расследование киберпреступлений, включая законодательные акты и деятельность специализированных органов. При разработке международных документов, Россия «предполагает уважение всех демократических норм применительно к данной сфере» [Бойко, 2023]..

1. **Законодательная база Российской Федерации**

- **Уголовный кодекс РФ**: статьи, предусматривающие ответственность за незаконный доступ к компьютерной информации, создание, использование и распространение вредоносного программного обеспечения и другие киберпреступления [УК РФ, 1996].
- **Федеральный закон "О информации, информационных технологиях и о защите информации"**: регулирует вопросы обработки и защиты информации в информационно-телекоммуникационных системах [Об информации, 2006].
- **Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ:** регулирует обработку персональных данных и включает в себя меры по их защите от незаконного доступа [О персональных, 2006]
- **Федеральный закон "О противодействии терроризму" (№ 53-ФЗ от 28 марта 2018 года):** этот закон внес изменения в ряд законов и ввел новые меры по борьбе с терроризмом в киберпространстве [О противодействии, 2018].

- Другие нормативные акты, регулирующие вопросы кибербезопасности на различных уровнях.

2. **Основные органы, занимающиеся борьбой с киберпреступностью в России**

- **МВД РФ**: департаменты и подразделения, специализирующиеся на киберпреступлениях.
- **ФСБ РФ**: центры по борьбе с киберугрозами и кибершпионажем.
- **Роскомнадзор**: регулирование вопросов связанных с интернетом и защитой персональных данных.

За рубежом, как и в России, киберпреступность признается одной из ключевых угроз безопасности. Различные страны разрабатывают и внедряют свои методы и стратегии борьбы с этим явлением, учитывая свои национальные особенности, уровень технологического развития и международные обязательства.

1. **Законодательная база ключевых зарубежных стран**

- **США**: Computer Fraud and Abuse Act (CFAA - закон о компьютерном мошенничестве и злоупотреблениях), законы о защите критической инфраструктуры, законы о защите персональных данных.
- **Европейский Союз**: Общий регламент по защите данных (GDPR), Директива о сетевой и информационной безопасности (NIS).

2. **Основные органы и международные организации, занимающиеся борьбой с киберпреступностью за рубежом**

- **США**: Федеральное бюро расследований (FBI), Агентство национальной безопасности (NSA), Cybersecurity and Infrastructure Security Agency (CISA).
- **Европейский Союз**: Европол, ENISA (Европейское агентство по сетевой и информационной безопасности).
- Международные инициативы и партнерства, такие как Группа G7 по кибербезопасности, ООН и ее подразделения по кибербезопасности.

Сравнивая опыт России и зарубежных стран в борьбе с киберпреступностью, можно выявить как общие тенденции и подходы, так и уникальные осо-

бенности, обусловленные национальными, культурными и технологическими факторами [Иванова, Ильиченкова, 2023]

Сходства в подходах:

Законодательная база: как в России, так и во многих зарубежных странах существует строгая законодательная база, регулирующая сферу киберпреступности. Это включает в себя уголовные и административные нормативы, направленные на пресечение незаконного доступа к информации, кибершпионаж, кражу личных данных и другие формы киберпреступлений.

Специализированные органы: как в России, так и за рубежом, существуют специализированные органы, ответственные за борьбу с киберпреступностью. Эти органы проводят мониторинг, анализ, и расследование инцидентов, а также сотрудничают с другими правоохранительными, государственными и частными структурами.

Международное сотрудничество: борьба с киберпреступностью требует глобального подхода. Россия и зарубежные страны активно участвуют в международном сотрудничестве, обмениваясь информацией о киберугрозах и координируя действия в расследованиях. В целях увеличения эффективности борьбы с киберпреступностью, принимаются международные нормативные акты в сфере кибербезопасности, среди таковых можно выделить следующие:

Резолюция Генеральной Ассамблеи ООН A/RES/73/266 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (2018 г.) - призывает государства к ответственному поведению в киберпространстве и укреплению доверия путем обмена информацией [Резолюция, 2018].

Парижское соглашение о доверии и безопасности в киберпространстве (2018 г.) – добровольные обязательства государств по обеспечению мира и стабильности в киберпространстве [Парижское, 2018].

Руководящие принципы ОЭСР по управлению рисками для цифровой безопасности на государственном уровне (2019 г.) – рекомендуемые меры политики в сфере кибербезопасности [Руководящие, 2019].

Резолюция ГА ООН A/RES/74/247 о достижениях в информатизации и телекоммуникациях (2020 г.) – осуждает использование ИКТ в преступных и террористических целях [Резолюция, 2020].

Видно, что на международном уровне основной упор делается на добровольных обязательствах государств, обмене информацией и выработке общих подходов. Жесткие обязывающие соглашения пока отсутствуют, тем более, в условиях существования экономических санкций против России.

Различия в подходах

- **Приоритеты в области кибербезопасности**: в то время как в России акцент делается на борьбу с внутренними угрозами и защиту критически важной инфраструктуры, западные страны фокусируются на кибершпионаже и кибертерроризме.
- **Степень государственного контроля:** в некоторых зарубежных странах существует более выраженная роль частного сектора в обеспечении кибербезопасности. В России же государственные органы, такие как ФСБ, занимают центральное место в этом процессе.
- **Культурные и правовые особенности:** в России, культурные и правовые особенности могут отражаться в подходе к регулированию и контролю в киберпространстве. В контексте культуры, сохранению традиционных ценностей и национальной идентичности, государственная безопасность может восприниматься как приоритет, что может отразиться в жестком контроле и мероприятиях для предотвращения киберугроз. В правовом аспекте, законы могут быть ориентированы на поддержание стабильности и предотвращение потенциальных угроз национальной безопасности. Как подчеркивает С. Бойко «основными противоречиями стали различия во взглядах на оценку угроз информационной безопасности, а также возможность отнесения к таким угрозам использование информационных и коммуникационных технологий (ИКТ) для достижения военно-политических целей, не совместимых с задачами обеспечения международного мира и безопасности» [Бойко, 2016].

Следует обозначить принципиальные различия в соблюдении прав человека в России и зарубежных странах. В России больший акцент делается на национальной безопасности и защите пользователей от опасного или нежелательного контента. Конституция гарантирует тайну переписки, но допускает ограничения прав граждан по мотивам безопасности. Например, законодательство по «суверенному Рунету» и «фейковым новостям» вызывают опасения о чрезмерном контроле и цензуре. Закон о личных данных также может быть использован как инструмент надзора. Такой фактор, как патернализм власти, также склоняет к принятию жестких мер контроля.

В любом случае, вопрос соблюдения прав человека в контексте обеспечения информационной безопасности остается одним из наиболее дискуссионных как в России, так и в глобальном масштабе. Поиск оптимального баланса – это постоянный процесс, требующий взвешенного и ответственного подхода со стороны государства и задействованных сторон.

В отличие от России, на Западе больший акцент делается именно на защите основных прав и свобод граждан при обеспечении безопасности в киберпространстве. Во многих западных странах действует жесткое законодательство о защите личных данных и неприкосновенности частной жизни пользователей интернета. Например, Общий регламент ЕС по защите данных (GDPR) налагает существенные ограничения на сбор и использование персональной информации как госорганами, так и частными компаниями.

При этом масштабная слежка, характерная для таких структур как АНБ в США, часто подвергается резкой критике со стороны гражданского общества и специальных правозащитных организаций. Например, Американский союз защиты гражданских свобод (ACLU) неоднократно подавал в суд на разведывательные органы США за нарушение Конституции. В западных демократиях существует определенный баланс интересов национальной безопасности и гражданских прав, хотя нахождение этого баланса – непростая задача. Тем не менее, в целом права человека в киберпространстве защищаются намного жестче, чем в России [Мордвинов, Удавихина, 2022].

Технологический прогресс играет двойственную роль в контексте киберпреступности: с одной стороны, он создает новые угрозы и возможности для преступников, с другой – предоставляет инструменты для борьбы с этими угрозами. Технологические инструменты играют ключевую роль в современной борьбе с киберпреступностью. Однако их эффективность во многом зависит от правильной настройки, интеграции с другими системами и постоянного обновления. Также важно помнить, что технология сама по себе не является панацеей, и ее использование должно быть частью комплексной стратегии кибербезопасности [Мордвинов, Удавихина, 2022]. Учитывая трансграничный характер многих киберпреступлений, крайне важно усилить международное сотрудничество. Это подразумевает создание общих стандартов, платформ для обмена данными и координации действий разных стран. Параллельно с этим, необходимо акцентировать внимание на образовании и подготовке специалистов. Учитывая быстрое развитие киберпространства, законы должны оперативно реагировать на новые формы и методы киберпреступлений. Важно подчеркнуть роль частного сектора. Государственные структуры, действуя в сотрудничестве с частными компаниями, исследовательскими центрами и экспертами, могут создать более гибкую и эффективную систему защиты от киберугроз, опираясь на наличие большего спектра неформальных возможностей защиты информационного пространства.

Библиографический список

1. Бойко С. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее. // Международная жизнь, 2016. – № 8 [Электронный ресурс] – Режим доступа: https://interaffairs.ru/jauthor/material/1718 (дата обращения: 30.11.2023).

2. Бойко С. Международная информационная безопасность: Россия в ООН. Начало истории (1998-2009 гг.). // Международная жизнь, 2023. – № 11. [Электронный ресурс] – Режим доступа: : https://interaffairs.ru/jauthor/material/1718 (дата обращения: 30.11.2023).

3. Иванова С. М., Ильиченкова З. В. Криминологические основы противодействия компьютерной преступности в экономике: учебн. пос. – Москва : РТУ МИРЭА, 2023. – 65 с. ISBN 978-5-7339-1717-7. [Электронный ресурс] – Режим доступа:. URL: https://e.lanbook.com/book/331643 (дата обращения: 29.11.2023).

4. Иванова А. В., Съедина Н. В. Глобальная военная безопасность. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспек-

ты, Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2023. – С. 527–536.

5. Золотухин В. М. Сохранение социокультурной идентичности в пространстве информационных войн. / В сборнике: Информационные войны как борьба геополитических противников, цивилизаций и различных этносов. Сборник трудов Всероссийской научной конференции. Под ред. В.Ш. Сабирова. 2018. – С. 231–239.

6. Золотухин В. М. Социокультурная идентичности и проблема информационной культуры в российской ментальности. / В сборнике: Информатика в философском и социальном аспектах. Сборник статей магистрантов и преподавателей КузГТУ. – Кемерово, 2020. – С. 80–85.

7. Золотухин В. М. Цифровые коммуникации и социокультурные риски в российской ментальности. / В сборнике: Социальные коммуникации: философские, политические, культурно-исторические измерения. сборник статей II Всероссийской научно-практической конференции с международным участием. – Кемерово, 2021. – С. 49–54.

8. Золотухин В. М., Логинова Г. Е. К вопросу о природе и сущности гибридной войны в современном мире: философско-культурологический аспект. // Вестник Кемеровского государственного университета культуры и искусств. 2017. – № 41-1. –С. 99–104.

9. Золотухин В. М., Степанцова Е. В. Социокультурный аспект правовой нормативности в России. // Вестник Кемеровского государственного университета культуры и искусств. 2015. – № 31. – С. 105–111.

10. Золотухин М. В., Михайлов В. Г. Цифровая экономика: проблемы, тенденции и перспективы. /В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты. Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2023. –С. 420–425.

11. Концепция стратегии кибербезопасности // Сайт Совета Безопасности РФ. 2013. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 17.11.2023).

12. Могилевцева К. А., Съедина Н. В., Филина А. А. Преступления против свободы, чести и достоинства личности: особенности уголовного законодательства разных стран. / В сборнике: Проблемы экономики и управления: социокультурные, правовые и организационные аспекты Сборник статей магистрантов и преподавателей КузГТУ. Кузбасский государственный технический университет имени Т.Ф. Горбачева. – Кемерово, 2022. – С. 467–474.

13. Мордвинов, К.В., Удавихина У.А. Киберпреступность в России: Актуальные вызовы и успешные практики борьбы с киберпреступностью. // Теоретическая и прикладная юриспруденция. — 2022. — № 1. — С. 83-88. — ISSN 2686-7834. [Электронный ресурс] – Режим доступа:. URL: https://e.lanbook.com/journal/issue/321824 (дата обращения: 29.11.2023).

14. Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция) // Собрание законодательства РФ. - 2006. - N 31 (часть I). - Ст. 3448.

15. О персональных данных" от 27.07.2006 N 152-ФЗ // Собрание законодательства РФ. - 2006. - N 31 (1 ч.). - ст. 3451.

16. "О противодействии терроризму" от 06.03.2006 N 35-ФЗ (последняя редакция) // Собрание законодательства РФ. - 2006.

17. Парижское соглашение о доверии и безопасности в киберпространстве. 2018. URL: https://pariscall.international/

18. Резолюция Генеральной Ассамблеи ООН A/RES/73/266 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». 2018. // Официальный сайт ООН [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/73/266 (дата обращения: 17.11.2023).

19. Резолюция ГА ООН A/RES/74/247 о достижениях в информатизации и телекоммуникациях. 2020 // Официальный сайт ООН. URL: https://undocs.org/ru/A/RES/74/247 (дата обращения: 19.11.2023).

20. Руководящие принципы ОЭСР по управлению рисками для цифровой безопасности на государственном уровне, 2019 // Официальный сайт ОЭСР URL: https://www.oecd.org/digital/digial-security-risk-management/ (дата обращения: 17.11.2023).

21. Степанцова Е. В. Геноцид: проблемы борьбы и предупреждения. / В сб.: Проблема фальсификации истории и реабилитации нацизма. Сб. мат. Международной научно-практической конференции. – Кемерово, 2023. – С. 171–178.

22. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. No 63: принят Гос. Думой 24 мая 1996 г.: одобр. Советом Федерации 5 июня 1996 г.: с изм. и доп. на 1 декабря 2022 г. // Собрание законодательства РФ.- 1996.-No 25.-Ст. 2954.

23. ENISA Threat Landscape 2020: Main incidents // European Union Agency For Cybersecurity, 2020. URL: https://www.enisa.europa.eu/ publications/enisa-threat-landscape-2020-main-incidents (дата обращения: 25.11.2023)

24. Zolotukhin V.M., Bikmetov R.S., Shiller V.V., Tarasenko A.A. Sociocultural aspect of criminal lam enforcement the russian mentality . Rudn conference on legal theory, methodology and regulatory practice (RUDN LTMRP conference 2021/ SHS Web of Conferences (см. в книгах). 2021. № 118. С. 02009

S. N. Kolchugino, D. A. Shitikov
Kuzbass State Technical University them. T.F. Gorbachev, Kemerovo, Russia

FEATURES OF THE FIGHT AGAINST CYBERCRIME IN RUSSIA AND ABROAD

supervisor: D. F. N., Professor of history, philosophy and social Sciences Zolotukhin V. M.

The article examines the issues of the emergence, spread and manifestation of cybercrime. Both similarities and differences in the fight against cybercrime in the field of Russian and foreign law enforcement have been identified. Attention is focused on the development of a unified law enforcement policy, socio-economic and other mechanisms in the fight against cybercrime. It is emphasized that the specifics of regional markets, legislative frameworks and cultural characteristics can influence the prevalence of one or another form of crime in a particular country.

Keywords: cybercrime, new technologies, social reality, digital space, identity fraud.