***Киберпреступность как новая угроза международной безопасности***

***Карасева Д.М.***

*Московский городской университет управления Правительства Москвы, Студент (бакалавр), 2024*

*E–mail: dashakara@yandex.ru*

Сегодня цифровая трансформация дипломатии, экономического развития и сотрудничества, а также других глобальных процессов ставит во главу угла вопросы международной безопасности. Наиболее острая проблема в этой связи – киберпреступность. Возможности несанкционированного доступа, широкий доступ к информации, удобство использования и неограниченное количество данных различного уровня конфиденциальности способствуют возникновению благоприятных условий для неправомерных действий в киберпространстве. Киберпреступность является критической угрозой для информационной безопасности государств [4], особенно злободневной данная тема воспринимается на международном уровне, когда происходит кража крупных сумм денег, баз данных с информацией о гражданах, и NFT-собственности, взламывают стратегически важные информационные системы с целью кражи информации особой важности.

Например, в последние годы растет доля информационно-коммуникационных технологий в преступлениях традиционного формата *(cyber enabled crimes)* и преступлениях, направленных на информационные технологии *(cyber dependent crimes)*. В Российской Федерации 34% преступлений совершено с использованием ИКТ [1]. С помощью иностранного ресурса Hackmageddon за 2022 г. было выявлено 3074 кибератак, что на 21 % больше по сравнению с 2539 кибератаками, выявленными в течение 2021 г., их число увеличивается с каждым днем [3].

В докладе изучается несколько кейсов: деятельность террористических группировок в Интернете, финансирование незаконных деяний криптовалютой, кража баз данных, киберпохищения и др. Отмечается, что террористические и идеологические кампании легче проводить в Сети, сложнее отслеживать их активность. Говоря о криптовалютных махинациях, возможно совершать такие преступления, как например, криптовымогательство. Преступники могут шифровать данные пользователя или заблокировать доступ к компьютеру, требуя выкуп в криптовалюте за восстановление доступа. Также, выявляется проблема защиты государственных данных, приводятся примеры сбоев государственных сайтов и утечки данных.

В условиях нарастающей угрозы киберпреступлений государства на площадке ООН на протяжении четырех лет [2] ведут переговоры о принятии Всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Заключительная сессия встреч Управления ООН по наркотикам и преступности закончилась 9 февраля 2024 г., но было заявлено, что потребуется больше времени для разработки документа, поскольку большое количество тонких формулировок требует согласования всех участников Комитета, в котором участвуют не только представители государств, но и международные организации и частные лица.

За последние годы выявлена тенденция по снижению общего количества традиционных и резкого повышения киберпреступлений, что делает данную сферу актуальной как с практической, так и научной точек зрения. Исследование обосновывает необходимость международного сотрудничества и координации действий в борьбе с киберугрозами, и продолжения переговоров по разработке единого документа на межгосударственном уровне.

**Источники и литература**

1. Доклад Министерства внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр» о состоянии преступности в России за январь-ноябрь 2023 г. URL: <https://media.mvd.ru/files/application/5040806>.
2. Хронология обсуждений Конвенции ООН о киберпреступности // Electronic Frontier Foundation URL: https://www.eff.org/ru/deeplinks/2023/04/un-cybercrime-treaty-timeline (дата обращения: 14.01.2024).
3. 2022 Cyber Attacks Statistics // HACKMAGEDDON URL: https://www.hackmageddon.com/2023/01/24/2022-cyber-attacks-statistics/ (дата обращения: 13.12.2023).
4. Kirilenko V.P., Alekseev G.V. Cybercrime and Digital Transformation. Theoretical and Applied Law. 2021;(1):39-53. <https://doi.org/10.22394/2686-7834-2021-1-39-53>.