

Виктимологические аспекты цифровой трансформации общества

А. А. Павлова, А. А. Николаева

Северо-Восточный федеральный университет им. М.К. Аммосова, г. Якутск, Россия

Аннотация. Статья посвящена виктимологическим аспектам цифровой трансформации общества в связи с высокими криминологическими рисками для пользователей информационно-коммуникационных технологий, необходимости активных разработок механизма обеспечения безопасности в киберсреде.

Ключевые слова: виктимологические аспекты, киберпреступность, цифровая трансформация общества, криминологические риски, кибербезопасность, киберсреда, кибержертва, кибервиктимология.

Victimological aspects of the digital transformation of society

A. A. Pavlova, A. A. Nikolaeva

M.K. Ammosov North-Eastern Federal University, Yakutsk, Russia

Abstract. The article is devoted to the victimological aspects of the digital transformation of society in connection with high criminological risks for users of information and communication technologies, the need for active development of a security mechanism in the cyber environment.

Keywords: victimological aspects, cybercrime, digital transformation of society, criminological risks, cybersecurity, cyber environment, cyber warfare, cybervictimology.

Постановка проблемы. В настоящее время мы живем в мире стремительно развивающихся технологий, в условиях новой реальности, так называемой пятой технологической революции. На данный момент пятая технологическая революция определена возникновением компьютеров, внедрением и развитием инновационных смарт-технологий. Вершиной данной эволюции стала сеть Интернет, которая дала возможность предельно облегчить процесс обмена информацией, а также обрести практически безграничные возможности получения больших объемов сведений в кратчайшие сроки. Проникая во все сферы человеческой жизнедеятельности, цифровизация влияет на огромное количество аспектов современного общества. Иными словами, процесс переноса подавляющей доли ключевых социально-политических функций общества в цифровую сферу представляется в качестве

ПАВЛОВА Арзулана Акрамовна – кандидат юридических наук, доцент, заведующий кафедрой «Уголовное право и процесс», Юридический факультет, Северо-Восточный федеральный университет имени М.К. Аммосова.

E-mail: arzulana@bk.ru

PAVLOVA Arzulana Akramovna – Candidate of Judicial Sciences, Associate Professor, Head of the Department of Criminal Law and Process of the Faculty of Law, M.K. Ammosov North-Eastern Federal University.

НИКОЛАЕВА Анастасия Анатольевна – магистрант, Юридический факультет, Северо-Восточный федеральный университет имени М.К. Аммосова.

E-mail: yktnastya@yandex.ru

NIKOLAEVA Anastasia Anatolyevna – Master's student, Faculty of Law, M.K. Ammosov North-Eastern Federal University.

логического и неотвратимого будущего. Несмотря на всю долгую историю цифровизации общества, одним из главных факторов, запустивших ее скорый процесс развития, стала **пандемия COVID-19**, когда был осуществлен перевод жизнедеятельности в режим онлайн, который существенно повлиял на цифровую трансформацию общества.

К. А. Айнутдинова отмечает, что повсеместное внедрение цифровых технологий во все сферы жизни способствует оптимизации и автоматизации рутинных задач и процессов, что ведет к улучшению и упрощению доступа к информации, новым цифровым продуктам и услугам, вследствие чего становятся очевидными потенциальные риски активно развивающейся цифровой среды, влекущие появление новых форм киберпреступности с уникальными схемами и недостаточно изученными способами совершения преступлений и создающие угрозы кибербезопасности для государственных органов, учреждений, бизнеса и отдельных граждан [1].

Согласно официальным статистическим данным за последние 10 лет наравне с развитием цифровых технологий активно растет и число преступлений с использованием различных информационных технологий, и сети Интернет (далее по тексту – киберпреступления). По данным ИЦ МВД РФ за январь-август 2023 года в России отмечается сохранение тенденции к увеличению количества киберпреступлений на 28, 7%. Их удельный вес в числе всех преступных посягательств возрос до 32, 9%, а по тяжким и особо тяжким – до 56, 4%. Больше всего совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29, 9%, в том числе совершенных с использованием сети Интернет – 28, 8%, расчетных (пластиковых) карт – 35, 7%¹.

Несмотря на то, что правоохранительными органами ведутся мероприятия по предотвращению киберпреступности параллельно идет и активное развитие способов и средств киберпреступников: разрабатываются новые схемы киберпреступлений, используются методы и технологии социальной инженерии с целью психологического воздействия на потенциальных жертв и манипулирования ими и т.п.

Кибержертвы – это отдельные лица или группы людей, которым причинен вред или ущерб в результате негативного информационно-психологического воздействия на них посредством определенных кибертехнологий (через интернет-пространство, с использованием сотовых телефонов, различных цифровых девайсов и гаджетов) [2].

Кибержертвой может стать любое лицо, как физическое, так и юридическое, в связи с чем факторы виктимности в данном случае будут иметь свои специфические признаки, в силу этого объединение их в одну релевантную группу представляется сложным.

Материалы, основанные на изучении виктимности киберпреступлений позволяют выделить следующие признаки личности кибержертв-физических лиц: доверчивость, наивность, рассеянность внимания, желание легкого обогащения, тревожность или недостаточный уровень информационной грамотности. Все эти факторы наиболее характерны для пожилого, или наоборот, молодого возраста, так как зачастую именно эти группы лиц обладают такими психологическими особенностями, являются наиболееязвимыми, поддаются манипуляциям и становятся легкой «добычей» для киберпреступников.

Если же говорить о юридических лицах – кибержертвах, таковыми они становятся в результате атак со стороны хакеров на операционную систему с целью незаконного получения конфиденциальных сведений или угрозу их уничтожения с целью выкупа. Основным рычагом воздействия на юридических лиц является то, что обладатели компьютерных систем несут ответственность за обработку большого количества персональных данных,

¹ <https://мвд.пф/reports/item/41741442/> (дата обращения: 10.02.2024 г.)

однако их клиенты могут стать жертвами киберпреступлений или их организации могут пострадать в результате преступных деяний в силу того, что им наносится ущерб в результате нанесения ударов по слабым местам компьютерной разработки или незаконного копирования и продажи компьютерных программ.

Литература

1. Айнутдинова К. А. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества// URL: https://kpfu.ru/staff_files/F_598192770/elibrary_Victimological_features_of_cybercrime.pdf
2. Известные ученые о кибервиктимологии // [Электронный ресурс]// -URL: <http://famous-scientists.ru/direction/163> (дата обращения: 03.06.2023).

References

1. Ajnutdinova K.A. Viktimologicheskie osobennosti kiberprestupnosti v usloviyah cifrovoj transformacii obshchestva// URL: https://kpfu.ru/staff_files/F_598192770/elibrary_Victimological_features_of_cybercrime.pdf
2. Izvestnye uchenye o kiberviktimologii // [Elektronnyj resurs]// -URL: «<http://famous-scientists.ru/direction/163>» (data obrashcheniya: 03.06.2023).