***Наместникова Мария Николаевна***
студентка
*Научный руководитель*
***Бобровникова Наталия Сергеевна***
старший преподаватель
ФГБОУ ВО «Тульский государственный
педагогический университет им. Л.Н. Толстого»
г. Тула, Тульская область

# ДОКСИНГ: ПОНЯТИЕ, ВИДЫ, ПРОФИЛАКТИКА

***Аннотация****: в статье анализируется феномен доксинга. Рассматриваются исторические предпосылки возникновения доксинга, начиная с 1990-х годов, и его эволюция в условиях цифровизации общества. Особое внимание уделяется классификации доксинга (деанонимизирующий, нацеливающий, делегитимизирующий), а также мотивам злоумышленников: месть, идеологические разногласия, кибербуллинг. В работе представлены некоторые меры профилактики доксига.*

***Ключевые слова****: доксинг, деанонимизирующий доксинг, нацеливающий доксинг, делегитимизирующий доксинг, деанонимизация, персональные данные.*

В современную цифровую эпоху доксинг стал распространенным явлением. Это связано с активным развитием интернета. С одной стороны, развитие интернета благотворно влияет на общество: общение в социальных сетях, способность самовыражения. Но, с другой стороны, интернет сделал приватность уязвимой, можно найти любую информацию о человеке: его данные, где он живёт, работает и многое другое.

Как явление доксинг возник в 90-х годах прошлого века. Первым системным раскрытием информации стало появление в 1997 г. специального веб-сайта под названием «Нюрнбергские файлы», на котором приводились данные (включая, адреса, телефоны и личные фото) около 200 человек, осуществлявших операции по искусственному прерыванию беременности (их называли

«абортивистами»). На сайте недвусмысленно предлагалось преследовать и убивать перечисленных граждан. Медицинская организация из штата Орегон «Planned Parenthood» обратилась с иском о запрете на распространение информации и блокировании сайта. После продолжительной судебной тяжбы в 2002 г. иск был удовлетворен Апелляционным судом 9-го округа США. Сайт вел активист Нил Хорсли [4, с. 68].

Пистолетов Д.А. в своей статье «Проблемы раскрытия личной информации в российском интернет-пространстве» дает следующее определение: «доксинг – получение личной информации о человеке (деанонимизация) и дальнейшее её распространение в открытых или закрытых источниках, а также среди групп людей» [1].Это может совершаться с целью травли, шантажа, либо как способ показать своё доминирование в интернете. Термин получен от названия сайта Doxbin – одного из наиболее известных сайтов для публикации личной информации других людей. На этом сайте публикуется личная информация несовершеннолетних, информация о других доксерах, информация о сотрудников государственных учреждений и организаций и не только.

Оксфордский британский и Всемирный словарь английского языка дает следующее определение доксингу: «поиск и опубликование личной или идентифицирующей информации о человеке во всемирной сети, как правило со злым умыслом» [7, с. 38].

Американский журналист Мэт Хонан один был одним из первых, кто, в своей статье «What is Doxind?» описал подробное происхождение этого термина. Он объяснил, что слово происходит от хакерского сленга «dropping dox», что в переводе с английского означает скинуть документы, то есть опубликовать личные данные соперника в отместку [6].

Лаборатория Касперского (международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и других киберугроз) выделяет следующую особенность доксинга, она заключается в том, что раскрываются персональные данные человека (настоящее имя, адрес, номер телефона, паспортные данные, банковские реквизиты, место

работы или учебы). Для этого используются открытые и закрытые источники информации: социальные сети, утечка базы данных. В отличие от физического пространства, информация в виртуальном распространяется мгновенно, и после первой публикации удалить ее из сети практически невозможно. Злоумышленники могут передать информацию о жертве ее родственникам, друзьям, преподавателям или работодателю.

Типология по целям доксинга разработана Дэвидом Дугласом, доктором Университета Квинсленда. Он профессионально исследует вопросы компьютерной этики и ответственных инноваций, а также взаимодействия общества и технологий. Целью злоумышленника в этом подходе является нанесение ущерба анонимности, неизвестности или репутации жертвы. В своих работах он выделил следующие типы:

− деанонимизирующий доксинг;

− нацеливающий доксинг;

− делегитимизирующий доксинг [2, с. 204].

Деанонимизирующий доксинг подразумевает собой сбор и публикацию личной информации с целью нарушения анонимности жертвы. Потеря анонимности может мешать экономическим, личным, академическим и профессиональным стремлениям личности, так как анонимность дает людям определенную защиту и свободу действий. К такому виду доксинга может относиться публикация настоящего имени, телефона, почты.

Нацеливающий доксинг – вид доксинга, который похож на предыдущий, но отличается тем, что при нем происходит публикация точных данных о физическом местонахождении человека – адреса или места проживания. Чаще всего этот вид представляет собой следующий этап после деанонимизации жертвы. Его отличие заключается в том, что он упрощает физический контакт с жертвой, переводит конфликт в реальную жизнь.

Делегитимизирующий доксинг – публикация конфиденциальных или ранее неизвестных данных с целью нанесения ущерба репутации и авторитету личности.

Существует несколько причин возникновения доксинга. Самая распространённая – месть. Из-за чувства несправедливости, люди стремятся отомстить своим обидчикам, раскрыв их личные данные. Это является опасной формой доксинга, поскольку может привести к преследованиям, угрозам и даже к физическому насилию.

Следующая причина – идеологические соображения. Это может включать в себя преследование отдельных лиц или групп, которые придерживаются противоположных взглядов или убеждений. В этом случае доксер может считать, что раскрытие личной информации о жертве поможет подорвать доверие к ней или лишить её поддержки. Этот тип доксинга часто связан с политическими или социальными целями.

Наконец, онлайн-тролли часто занимаются доксингом ради развлечения. Они получают удовольствие, сея хаос и страдания среди своих жертв, и доксинг – лишь один из многих способов, с помощью которых они это делают. К сожалению, последствия доксинга могут быть серьёзными и непоправимыми: жертвы подвергаются преследованиям, угрозам и даже физическому насилию [3].

«Лабораторией Касперского» были предложены некоторые рекомендательные меры профилактики феномена.

1. В первую очередь следует повысить осведомлённость о данной проблеме среди сотрудников правоохранительных органов, чтобы снизить эффективность деятельности хакеров, поскольку именно их неосведомлённость является главной причиной, по которой хакеры в принципе прибегают к подобным действиям. Сделать это можно с помощью различных мероприятий: конференций, повышения квалификации, распространения среди сотрудников информации на рабочем месте.

2. Повысить осведомлённость педагогов о данной проблеме, поскольку доксеры нередко могут написать именно в место обучения школьника либо студента, чтобы вызвать негативное отношение у тех людей, с которыми контактирует молодой человек. Подобные практики действительно могут вызвать

психологические травмы. Также возможно проведение классных часов и иных мероприятий, на которых педагоги смогут повысить осведомлённость самих обучающихся о данной проблеме. Им следует знать о том, как эффективно противостоять доксерам, чтобы не дать им успешно реализовать задуманное.

3. Распространять информацию о проблеме и методах борьбы с ней посредством средств массовой информации. Если повышение осведомлённости сотрудников правоохранительных органов повысит их компетенцию в борьбе с такими правонарушениями, а повышение осведомлённости обучающихся повысит информированность молодого поколения, то публикации в СМИ и иных ресурсах смогут повысить осведомлённость общества о проблеме в целом [1].

Результаты исследования, проведенного «Лабораторией Касперского» в 2021 году, выявили, что около 20% пользователей приложений для знакомств в сети столкнулись с доксингом. В 2020 году аналогичный опрос, организованный той же компанией, продемонстрировал, что 64% россиян предпринимали попытки удалить свои персональные данные с различных веб-ресурсов и социальных платформ. При этом, по словам каждого пятого респондента, в интернете обнаруживались сведения о них или их родственниках, которые они предпочли бы видеть конфиденциальными. Анализ этих данных позволяет утверждать, что доксинг представляет собой не просто нарушение личного пространства, но и потенциальную опасность для безопасности. Для снижения вероятности подобных инцидентов требуется всесторонний подход к защите личной информации.

***Список литературы***

1. Пистолетов Д.А. Проблемы раскрытия личной информации в российском интернет пространстве / Д.А. Пистолетов [Электронный ресурс]. – Режим доступа: https://mgpu-media.ru/issues/issue-60/sotsiologicheskie-issledovaniya/problema-raskrytiya-lichnoj-informatsii-v-rossijskom-internet-prostranstve.html (дата обращения: 06.05.2025).

2. David M. Douglas. Doxing: a conceptual analysis // 28 June 2016. P. 204.

3. Статьи Брайан М. Вулф [Электронный ресурс]. – Режим доступа: https://www.techradar.com/author/bryan-m-wolfe (дата обращения: 06.05.2025).

4. Романовская Е.А. Публично-правовые основы противодействию доксинга / Е.А. Романовская // Наука. Общество. Государство. – 2023. – №2. – С. 68. DOI 10.21685/2307-9525-2023-11-2-7. EDN RPCHZR

5. Что такое доксинг и как от него защищаться [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/doxing-methods/30598/ (дата обращения: 06.05.2025).

6. Mat Honan What Is Doxing? [Electronic resource]. – Access mode: https://www.wired.com/2014/03/doxing/ (date of request: 06.05.2025).

7. Федоров Р.В. Теоретико-правовые аспекты права на анонимность в сети Интернет / Р.В. Федоров // Юридический вестник ДГУ. – 2022. – №4. – С. 38. DOI 10.21779/2224-0241-2022-44-4-34-41. EDN GQBOOK