Секция «Информационное общество, цифровая экономика и информационная безопасность»

Противодействие фейковым новостям как механизм обеспечения информационной безопасности

Научный руководитель – Зуева Анна Сергеевна

Макаева Лиана Аслановна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия
E-mail: liana.makaeva2013@yandex.ru

Информационная безопасность— практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных.

Фейковая новость- это информационный вброс, содержащий в себе специально подготовленную информацию заведомо провокационного и резонансного характера. При этом сам фейк может содержать как заведомо ложную, так и истинную (проверяемую) информацию, вырванную из контекста конкретной беседы, разговора или выступления. Цель фейковой новости - создание ажиотажа вокруг мнимого информационного повода, создаваемого вбросом заведомо провокационной информации, имеющей резонансный характер. Основной задачей фейковой новости при этом становится перехват информационной повестки и замыкание ее на себя, с тем, чтобы содержание фейка на некоторое время стало навязчивой идеей, подчиняющей себе сознание человека, подпавшего под влияние фейковой новости.

В Госдуму РФ внесен пакет законопроектов, направленных на борьбу с недостоверной информацией, публикуемой под видом общественно значимых достоверных сообщений. За распространением в СМИ и интернете фейков, создающих угрозу жизни гражданам, предлагается установить штраф до 1 миллиона рублей. По мнению опрошенных юристов, в новом законопроекте учтен актуальный зарубежный опыт в вопросе обеспечения общественной информационной безопасности в интернете. При этом в плане гуманности и соразмерности наказаний опасности правонарушения российский законопроект качественно превосходит свои зарубежные аналоги.

Авторы законопроекта отмечают, что «неконтролируемое распространение недостоверной информации, распространяемой под видом достоверных сообщений, может. . . создать реальную опасность жизни и здоровью граждан, привести к массовым беспорядкам, создать угрозу государственной, общественной или экологической безопасности».

Рассмотрим основные методы борьбы с недостоверной информацией, публикуемой под видом общественно значимых достоверных сообщений.

Штрафы за распространение недостоверной информации (фейки) в интернете. Новый законопроект предусматривает за распространение фейков, создающих угрозу жизни штраф для граждан в размере 3-5 тыс.руб., для должностных лиц - 30-50 тыс.руб., для юридических лиц — от 400 тысяч до 1 миллиона рублей.

Защита государственных интересов в сети. В нынешнем законопроекте предусмотрена возможность принятия мер по ограничению доступа к материалам, выражающих в неприличной форме явное неуважение к обществу, государству, официальным государственным символам России, Конституции РФ и органам власти.За такие правонарушения также будет установлена административная ответственность: за распространение в интернете - штраф в размере от 1-5 тыс.руб. или административный арест на срок до 15 суток.

Регулирование соцсетей по нормам законов о СМИ. Привлечение журналистов к ответственности. Блокировка аккаунтов и сайтов.

В 2012 году президентом РФ Владимиром Путиным был подписан № 139-ФЗ, вносящий в другие федеральные законы ряд положений, предполагающих фильтрацию интернет-сайтов по системе чёрного списка и блокировку запрещённых интернет-ресурсов. Согласно закону о досудебной блокировке сайтов, Генпрокуратура может добиваться блокировки сайтов, если обнаружит там призывы к массовым беспорядкам, осуществлению экстремистской деятельности и несогласованным акциям.

Персонализация пользователей соцсетей и блогеров. Временная блокировка соцсетей. В ноябре 2018 года Правительство РФ утвердило правила идентификации пользователей мессенджеров с помощью номера телефона. Сервисами смогу пользоваться лишь те, на кого оформлен номер. Ответственность за проверку информации о корректности номера будет лежать на администраторах мессенджера. Помимо этого мобильные операторы буду хранить данные о том, в каких приложениях переписываются их клиенты.

Блокировка мессенджеров и соцсетей. В октябре 2017 года было вынесено судебное решение в пользу ФСБ в связи с отказом руководством Telegram передавать ключи для расшифровки сообщений 6 лиц, обвиняемых в совершении теракта в Петербурге.20 марта 2018 года мессенджеру было предъявлено требование предоставить в течение 15 дней технологию дешифровки личных сообщений пользователей, которое не было удовлетворено.13 апреля 2018 года Таганский суд Москвы вынес решение в пользу Роскомнадзора, тем самым позволив начать блокировку мессенджера на территории России.

Раскрытие ключей шифрования. В марте этого года Федеральная служба безопасности (ФСБ) обязала «организаторов распространения информации» предоставлять в ведомство ключи шифрования в срок до 10 дней «со дня получения запроса». Приказ опубликован на официальном интернет-портале правовой информации.

Доступ к персональным данным. С 1 июля 2018 года в России вступил в силу закон Яровой, который обязывает операторов телекоммуникационных услуг хранить записи телефонных сообщений и интернет-трафик их клиентов на протяжении полугода.

Досмотр провайдеров. Согласно «закону Яровой» интернет-провайдерам нужно будет хранить текстовые сообщения, голосовую информацию, изображения, звуки, видео и другую информацию своих пользователей.

Блокировка анонимайзера. В России 1 ноября 2017 года вступил в силу закон, обязывающий владельцев VPN-сервисов и так называемых анонимайзеров закрывать доступ к запрещенным сайтам.Речь о запрете сервисов не идет.

Чтение переписки граждан. Министерство связи опубликовало проект приказа о требованиях к «организаторам распространения информации» в интернете.В приказе подробно перечислены те данные, которые «организаторы распространения информации» должны хранить в течение 6-12 месяцев и, самое главное, предоставлять специальным службам, ведущим оперативно-разыскную деятельность (ОРД).Обязанность хранить и предоставлять спецслужбам данные о нашей переписке была закреплена в законе «Об информации» еще в мае 2014 года.ОРС обязан хранить текстовые сообщения и иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента оконча-

ния их приема, передачи, доставки и (или) обработки. Эта норма вступила в силу с 1 июля 2018 года.

Кибердивизии.В апреле 2018 года секретарь Совета безопасности Николай Патрушев заявил, что в России необходимо создать институт так называемых «интернет-дружинников» из блогеров и волонтеров. Они усилят работу по патриотическому и духовно-нравственному воспитанию молодежи на Северном Кавказе, а также будут препятствовать распространению радикальных идей через интернет.