

Информационная безопасность для журналистов-расследователей

Научный руководитель – Черевко Тарас Сергеевич

Ларина Анастасия Александровна

Студент (бакалавр)

Московский государственный университет имени М.В.Ломоносова, Факультет журналистики, Кафедра новых медиа и теории коммуникации, Москва, Россия

E-mail: larinaanastasia2112@gmail.com

Журналисты-расследователи по всему миру рискуют стать жертвой физической расправы из-за своей профессиональной деятельности. За последние двадцать лет к этому риску добавились информационные угрозы. Главная задача этого исследования - выяснить, какие подходы и практики в сфере информационной безопасности используют российские журналисты и издания.

Для удобства мы разделили подходы к информационной безопасности на комплексный и некомплексный. Комплексным подходом мы будем считать регулярное использование мер, направленных на ее обеспечение. Некомплексным подходом мы будем считать наличие мер, которые применяются нерегулярно или затрагивают не все сферы цифровой среды.

В рамках исследования мы взяли интервью и комментарии у трех журналистов (Роман Анин, Андрей Захаров, Иван Голунов, Елена Милашина), а также задали вопрос двум экспертам (Ксения Ермошина - старшая научная сотрудница Центра Интернета и Общества CNRS; Сергей Смирнов - «Теплицы социальных технологий»), которые проводят тренинги в сфере информационной безопасности для журналистов. Все интервью были взяты в августе 2022 года.

На основе анализа интервью можно сделать вывод, что комплексный подход к информационной безопасности используют журналисты-расследователи, которые постоянно пишут на такие темы, как коррупция, офшоры и власть (Роман Анин и Андрей Захаров). Они осознают высокие риски из-за работы и тщательно следят за информационной безопасностью. Журналисты, работающие в основном с открытыми данными (Иван Голунов), используют только базовые меры цифровой защиты. Кроме того, два опрошенных журналиста интересовались информационной безопасностью как отдельной областью. Только один журналист имел персонального консультанта в этой сфере, так как это было жизненно важно из-за больших рисков (Елена Милашина).

Из анализа интервью следует, что многие российские издания, к сожалению, используют некомплексный подход к информационной безопасности. Комплексный подход использует Meduza (*признано СМИ-иноагентом), ВВС и «Важные истории» (*признано нежелательной организацией). Это обусловлено тем, что эти издания специализируются на жанре расследований. Журналисты, сотрудничающие с ними, испытывают больше рисков, чем сотрудники, таких СМИ, как Коммерсант или РБК.

По итогам интервью с журналистами и экспертами был составлен гайд по информационной безопасности для журналиста-расследователя. Он состоит из восьми пунктов, каждый из которых затрагивает один из аспектов работы журналиста над расследованием.

Кратко обозначим основные принципы информационной безопасности для журналиста-расследователя из составленного нами гайда:

1. Разделение устройств для работы и личной жизни;

2. Шифрование данных (при их хранении на диске, а также передаче - по почте или через мессенджеры);
3. Общение с источниками только через мессенджеры со сквозным шифрованием;
4. Регулярное обновление паролей на устройствах и аккаунтах, сложный подбор паролей;
5. Отказ от разблокировки устройств по отпечатку пальца или face-ID;
6. Безопасный поиск информации в Интернете с использованием сервисов VPN;
7. Ограничение распространения информации в социальных сетях;
8. Журналист должен объяснить своим близким и семье базовые методы информационной безопасности, чтобы устранить возможные риски для них.