

ИНФОРМАЦИОННЫЕ АГЕНТСТВА И СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ВЫЗОВЫ

В настоящее время по всему миру функционирует более ста крупных информационных агентств.

Мой личный многолетний опыт работы в информационном агентстве ТАСС, регулярные встречи с руководителями мировых новостных медиа и участие в международных форумах позволяют мне говорить о том, что все информационные агентства сталкиваются в своей деятельности с одними и теми же вызовами.

Одним из самых существенных вызовов является рост киберпреступлений, который остаётся несомненной угрозой коллективной безопасности.

В 2016 году по всему миру было зафиксировано порядка 1,5 миллионов кибератак, иначе говоря – более 4000 в день.

Нынешний уровень развития информационных сетей позволяет говорить о формировании единого информационного пространства, в котором поставщик и потребитель информации находятся в режиме взаимодействия в реальном времени.

Возрастающая скорость передачи данных и структурное развитие информационных сетей, с одной стороны, непрерывно делают процесс передачи и обработки информации всё более оперативным. Однако с другой стороны, рост влияния и увеличение охвата информационных сетей делают их всё более привлекательными для преступников.

Интернет-пространство всё чаще используется террористическими организациями как площадка для пропаганды экстремистских взглядов и даже вербовки в свои ряды.

Нередко подобными площадками становятся социальные медиа, обладающие большой аудиторией и при этом не всегда способные обеспечить контроль размещаемого в них контента.

Специфика социальных медиа, предоставляющая каждому желающему возможность высказаться, вне зависимости от его компетентности в вопросе,

подчас способствует, таким образом, росту напряжённости в информационном пространстве.

Современные информационные агентства, будучи важной составной частью мировых информационных сетей, также подвержены опасности со стороны киберпреступников. Однако здесь это, в первую очередь, фейковые вбросы провокативных сообщений.

Роль, которую играют информационные агентства в формировании новостной картины мира, чрезвычайно велика. Оперативно генерируя информацию и предоставляя её СМИ, информационные агентства являются одним из ключевых звеньев в эффективном функционировании мирового сообщества.

И тем опаснее ситуации, в которых в результате хакерских атак агентства публикуют заведомо ложную информацию. В лучшем случае преступники ограничатся самим взломом, в худшем – размещённое сообщение может послужить катализатором международного конфликта. Ещё в 2009 году генеральный секретарь Международного союза электросвязи ООН Хамадун Туре заявил, что в случае третьей мировой войны последняя будет проходить в киберпространстве.

Как известно, фейковые вбросы способны и навредить репутации информационного агентства, и даже дестабилизировать политическую обстановку.

Возникает вопрос: как можно противостоять киберпреступникам?

Во-первых, обеспечение безопасности мирового информационного пространства немислимо без проработки международных положений в этой сфере. На данный момент у мирового сообщества отсутствует единая программа по противодействию киберугрозам. Необходимость принятия подобной программы ощущается всё острее с каждым годом. Примечательно, что Россия выступала с подобной инициативой в адрес ООН и США ещё в 1998 году.

Тем не менее, ряд программ функционирует на уровне международных организаций и отдельных стран. Так, в 2001 году в Будапеште была подписана Европейская конвенция по киберпреступлениям.

В 2011 году в рамках ШОС Россией, Китаем, Таджикистаном и Казахстаном было ратифицировано соглашение о сотрудничестве в области информационной безопасности.

Россия выступает в качестве одного из центров по противодействию киберпреступности. 5 декабря 2016 года Указом Президента РФ была утверждена Доктрина информационной безопасности Российской Федерации, в которой борьба с киберугрозами тесно связана с обеспечением национальной безопасности.

Обсуждается проект Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, в которой особое место уделено безопасности и достоверности информации.

22 января 2017 года вступило в силу соглашение между Россией и Индией о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий.

Помимо реализации соответствующих программ на государственном уровне необходима и разработка самими информационными агентствами средств защиты от хакерских взломов.

Привлечение специалистов в сфере IT и формирование специализированных подразделений внутри агентств будет способствовать созданию актуальных систем защиты, блокирующих попытки проникновения преступников и обеспечивающих сохранность передачи данных.

Параллельно с этим необходимо постоянное совершенствование систем контроля публикуемого контента.

Скорость передачи информации обязывает информационные агентства оперативно отслеживать все неточности и искажения в материале. С учётом угрозы фейковых вбросов агентствам необходимо сообща подумать о механизме «срочной информационной кнопки», срочной проверки информации.

Также немаловажным является понимание кибербезопасности как неотъемлемой части корпоративной культуры, что подразумевает обучение персонала правилам безопасной работы с информацией. В ряде случаев преступники могут воспользоваться внутренними аккаунтами сотрудников агентства с целью доступа к корпоративной информации.

Современное информационное агентство немисливо без полноценного веб-сайта. Публикуемые на новостных сайтах материалы мгновенно расходятся по всему миру. Участвовавшие случаи DDoS-атак, приводящих к затяжным сбоям в работе, обязывают нас поддерживать в актуальном виде защиту собственных новостных сайтов.

Наконец, как показывают многочисленные примеры выше, информационным агентствам необходимо уделять особое внимание вопросам безопасности при работе с социальными медиа, особенно уязвимыми к хакерским атакам. Это включает в себя и элементарные меры по созданию сложных паролей в аккаунтах, и налаженные каналы связи с соответствующими подразделениями сервисов, с которыми мы взаимодействуем.

Уверен, что, используя вышеописанные методы и придерживаясь мировых стандартов информационного контроля и безопасности, информационные агентства смогут успешно противостоять всем вызовам, которые бросает им непростая и бурно меняющаяся ситуация в мире.