Информационная безопасность: как распознать фейки и защитить себя от психологического воздействия

В условиях современных вызовов информационное пространство становится полем для психологического воздействия.

Цель таких кампаний — посеять панику, подорвать доверие к органам государственной власти и Вооруженным Силам, а также сорвать мероприятия гражданской обороны.

Чтобы обеспечить устойчивость системы управления и личную безопасность, необходимо знать механизмы работы дезинформации и алгоритмы действий при ее обнаружении.

Как распознать фейк: тревожные сигналы

Противник использует отработанные сценарии, которые легко вычислить, если сохранять критическое мышление:

- **Эмоциональный шантаж и паника.** Сообщения начинаются со слов «Срочно!», «Шок!», «Все в панике!», «Это скрывали!». Фейки всегда бьют по эмоциям, чтобы отключить логику.
- **Подмена источника.** Взломанные аккаунты официальных лиц, поддельные сайты-двойники (отличающиеся одной буквой в адресе) или публикации от имени «анонимных инсайдеров» и «очевидцев». **Фальшивые документы.** Сообщения с грифами «секретно», «утечка», «внутренний приказ». Настоящие документы публикуются только на официальных ресурсах с указанием входящих номеров, печатей и корректных подписей.
- **Технологические уловки.** Использование дипфейков — аудио- и видеоподделок, имитирующих голоса и лица руководителей, с призывами не эвакуироваться или идти в ложном направлении.
- **Визуальный обман.** Старые фотографии и видео выдаются за свежие. Проверить их можно через обратный поиск по картинке.
- **Призывы к немедленному действию.** Требования «срочно распространять», бежать к банкоматам (при фейках о заморозке вкладов) или собираться в местах, создающих заторы на реальных маршрутах эвакуации.

Что делать при столкновении с дезинформацией

Если вы получили тревожное сообщение в мессенджере, соцсетях или увидели подозрительную новость, следуйте четкому алгоритму:

1. **Не пересылать и не комментировать.** Любой репост или даже гневный комментарий разгоняет алгоритм соцсетей и помогает фейку охватить новую аудиторию.
2. **Включить критическое мышление.** Отделите эмоции от сухих фактов. Если новость представляет собой «живую историю человека» без логической подводки — это повод для проверки.
3. **Проверить первоисточник.** Найдите эту информацию на официальных ресурсах: сайтах правительства, ведомств, в государственных СМИ и верифицированных аккаунтах в мессенджерах. Если в поисковике новость выдает только сомнительные каналы — она сфабрикована. **Сверить детали.** Проверьте адрес сайта на наличие лишних букв, а в аудиосообщениях — на неестественные интонации. При проверке документов обращайте внимание на фамилии должностных лиц и официальные реквизиты .
4. **Воспользоваться официальными алгоритмами опровержения.** О факте распространения дезинформации необходимо сообщить в компетентные органы. Для этого в системе гражданской обороны развернуты дополнительные каналы приема обращений через **единый номер «112».**
5. **Дождаться официального опровержения.** Достоверную информацию о сбоях, эвакуации или работе финансовых систем публикуют по всем защищенным каналам одновременно: через СМС-рассылку операторов, громкоговорящую связь, домофоны, сайт МЧС/администрации и верифицированные мессенджеры.
6. **Если вы сомневаетесь** в подлинности новости или сообщения — не полагайтесь на одну ссылку или пересланный текст. Обязательно уточните информацию по резервному каналу: позвоните по номеру 69-00-05, доб. 251 (Старший группы Комитета гражданской обороны и защиты населения Республики Марий Эл).

Помните: главная задача противника — лишить вас четкой картины происходящего. Доверяйте только проверенным данным, сохраняйте спокойствие и помогайте выявлять информационные вбросы, сообщая о них по номеру 112.