

М. В. Тумбинская, канд. техн. наук, Казанский национальный исследовательский технический университет им. А. Н. Туполева — КАИ (КНИТУ-КАИ), г. Казань, tumbinskaya@inbox.ru

Защита информации в социальных сетях от социоинженерных атак злоумышленника

В настоящее время пользователи активно используют социальные сети, то есть являются открытым источником информации для злоумышленников, которые могут реализовать социоинженерные атаки, например, распространение таргетированной информации. В статье предложена формализация обобщенного алгоритма распространения таргетированной информации, методика защиты от таргетированной информации в социальных сетях, позволяющие повысить уровень защищенности персональных данных пользователей социальных сетей.

Ключевые слова: информационная безопасность, социальная информационная система Social Network, таргетированная информация, злоумышленник, сценарий атаки.

Введение

На сегодняшний день каждый человек является пользователем интернет-пространства, активно развиваются виртуальные социальные сети — *Online Social Network (OSN)*. В литературе в качестве синонима понятия «социальные сети» также используется понятие «микроблогинг». Применение социальных сетей в различных сферах деятельности описано в источнике [1]. Социальные сети характеризуются простотой реализации продвижения бизнеса, распространения рекламы товаров и услуг, простотой организации досуга, хобби, личного общения и обмена информацией, одновременно являясь открытым источником информации для злоумышленников. Обзор киберпреступников и кибермошенников представлен в работах [2–6]. Как правило, злоумышленники в *OSN* для достижения своих целей применяют мошеннические схемы, что подтверждается исследованиями [7–8]. Авторы [9–10] рассматривают различные способы мошенничества в наи-

более распространенных социальных сетях *Facebook*, *Whatsapp*, *Twitter* и т. д., методы и способы борьбы с ними.

Злоумышленники в качестве одного из способов получения конфиденциальной информации используют распространение таргетированной информации [11] в социальных сетях на основе методов манипуляции пользователями [12–15] и социальной инженерии. Понятие таргетированной информации порождено понятием «таргетированная реклама». Исследования, посвященные таргетированной рекламе в социальных сетях, представлены в работах авторов [16–19]. Вопросы распространения информации в системах микроблогинга рассмотрены в работе [21]. Модель поведения пользователей в системах микроблогинга рассмотрена в работе [20]. Под таргетированной информацией понимается нежелательная информация, содержащаяся в информационных сообщениях пользователя или группы пользователей (сообщества) социальной сети [22]. Для своих целей злоумышленники могут использовать лиде-