УДК 343.985.8

А.В. Балиткин

ИСПОЛЬЗОВАНИЕ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ПРИ ДЕАНОНИМИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ МЕССЕНДЖЕРОВ С ЦЕЛЬЮ РЕШЕНИЯ ЗАДАЧ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Анализ современного состояния правоприменительной практики позволяет выявить тренд роста использования информационно-коммуникационных технологий в преступной деятельности. Сервисы мгновенного обмена сообщениями со встроенными алгоритмами шифрования обосновались в списках используемого злоумышленниками программного обеспечения по ряду причин, основными из которых являются: повсеместность использования, возможность взаимного удаления данных, условная анонимность пользователей (в том числе сложность их деанонимизации).

Действительно, в современных условиях динамично развивающегося информационного поля, используемого преступниками для разработки новых методов анонимизации и противодействия правоохранительным органам, их идентификация усложняется, а получение оперативной информации о личности злоумышленников становится важной проблемой, требующей разработки научных рекомендаций в виде универсальных тактических приемов.

Одним из инновационных способов решения данной проблемы, должным образом не освещенным в научной литературе по отношению к другим, может выступать использование методов социальной инженерии, оперирующей понятием «социо-психологические манипуляции», которые применяются (в том числе преступниками) для получения доступа к защищенным компьютерным системам (включая мобильные устройства) с целью получения интересующей информации.

Обзор публикаций и тематических форумов в сети Интернет свидетельствует, что аналогичный термин присутствует в профессиональном сленге сотрудников правоохранительных органов – специалистов в сфере обеспечения информационной безопасности и встречается в научных исследованиях. Наиболее полно сущность данного термина, в том числе применительно к правоохранительной деятельности, в своих трудах рассматривает М.В. Губич, а его позиция использована нами в качестве основы для разработки научных рекомендаций, конечным результатом которых должно выступить решение определенных задач оперативно-розыскной деятельности (ОРД).

В зависимости от конкретно сложившейся ситуации, тактика и последовательность действий оперативных сотрудников будет различной, в связи с чем представить их исчерпывающий перечень в данной пубикации не представляется возможным. Вместе с тем в целях полноты исследования можно выделить основные приемы получения информации об интересующем лице (деанонимизации), отразив кратко их сущность.

Первый прием, используемый оперативным сотрудником, направлен на введение интересующего лица в заблуждение и понуждение к выполнению необходимых для его деанонимизации (идентификации) действий.

Второй прием также характеризуется активностью оперативного сотрудника, однако она направлена на создание для интересующего лица таких обстоятельств (или их видимости), при которых он инициативно выполняет действия в интересах оперативного подразделения, не подозревая об этом.

Таким образом, использование методов социальной инженерии при деанонимизации пользователей мессенджеров в целях решения задач ОРД представляется перспективным направлением для научных исследований, широкое изложение результатов которого возможно в специализированных научных изданиях ввиду ограниченного распространения таких сведений.

УДК 004

П.Л. Боровик

НЕФОРМАЛЬНАЯ МОДЕЛЬ ВОЗМОЖНОГО ПРАВОНАРУШИТЕЛЯ В КОНТЕКСТЕ МОДЕРНИЗАЦИИ ВЕДОМСТВЕННОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время в органах внутренних дел (ОВД) проводится последовательная работа по модернизации ведомственной системы информационной безопасности (ИБ), основывающаяся на качественно новых подходах. Так, приказом Министерства внутренних дел Республики Беларусь от 30 сентября 2022 г. № 256 «О единой цифровой платформе Министерства внутренних дел» утверждены входящие в состав документированной информации в области обеспечения ИБ нормативно-методические документы, направленные: на определение парольной политики и организации порядка доступа к отдельным сегментам ведомственной сети передачи данных (ВСПД) ОВД; защиту от вредоносного программного обеспечения; криптографическую защиту информации; межсетевое экранирование периметра ВСПД ОВД; мониторинг, аудит событий ИБ и оперативное реагирование на инциденты безопасности; организацию резервного копирования информации и др.

В контексте широкого спектра рисков и угроз национальной безопасности в информационной сфере, обозначенного в Концепции национальной безопасности Республики Беларусь (утвержденной Указом Президента Республики Беларусь от