УДК 004.056.53

ДЕАНОН ПО ТЕЛЕГРАММУ

Таран Е.А., студент гр. ПИ2241, 2 курс магистратуры,
Трофименко М.С., студент гр. ПИ2241, 2 курс магистратуры,
Савинская Д.Н., к.э.н., доцент
Научный руководитель: Савинская Д.Н., к.э.н., доцент
Кубанский государственный аграрный университет им. И.Т. Трубилина
г. Краснодар

XXI век – век информации и информационных технологий. Ни для кого не секрет, что мир не стоит на месте, развивается, совершенствуется. В настоящее время у каждого современного человека есть странички (аккаунты) в различных социальных сетях (Instagram, VK, Facebook, Twitter и др.) на которых отражена жизнь этого человека, его стремления, увлечения, мнения и т.д. Помимо социальных сетей достаточно популярны различные системы мгновенного обмена сообщениями, т.е. мессенджеры, такие как WhatsApp, Viber, Telegram и др.

Доступность к личной информации дала толчок развитию различных видов преступной деятельности, с которыми сталкивается большое количество пользователей. Преступная деятельность в интернете, также известная как киберпреступность, охватывает широкий спектр незаконных и вредоносных действий, проводимых онлайн. Приведем несколько примеров киберпреступлений:

1. Фишинг – отправка мошеннических электронных писем или сообщений, которые кажутся законными, с целью украсть личные данные, такие как пароли и номера кредитных карт.

2. Распространение вредоносного программного обеспечения (вирусов, троянов, шпионских программ) – распространение программ, которые могут повредить компьютер, украсть личные данные или использовать зараженный компьютер для распространения самого вредоносного программного обеспечения.

3. Атаки типа «отказ в обслуживании» – намеренная перегрузка сервера или сети множественными запросами, что приводит к неработоспособности ресурса.

4. Интернет-мошенничество – включает в себя различные схемы, такие как аукционное мошенничество, мошенничество с использованием платежных систем и мошенничество с онлайн-кредитами.

5. Киберсталкинг – преследование или домогательства людей в интернете, включая угрозы, распространение личной информации и другие формы онлайн-преследований.

6. Кража идентичности – использование чужой личной информации без разрешения для совершения мошенничества или других преступлений.

7. Кибертерроризм – использование интернета для проведения террористических действий, таких как распространение пропаганды, координация атак или сбор средств для террористических групп.

8. Криптовалютные аферы – включают в себя различные виды мошенничества, связанных с криптовалютами, включая пирамиды, фишинговые атаки на кошельки криптовалют.

Эти примеры представляют собой лишь некоторые из множества возможных форм киберпреступлений. По мере развития технологий и интернета появляются и новые виды киберугроз.

Как правило киберпреступления совершаются с анонимных аккаунтов, что создает особую сложность в раскрытии данного вида преступлений, учитывая при этом высокий уровень защиты переписки и конфиденциальности пользователей в мессенджерах.

Рассмотрим деанонимизацию, которая, по своей сути, является одной из форм киберпреступления, как способ раскрытия «анонима-преступника». Применение деанонимизации в борьбе с киберпреступностью может быть оправданным в случаях, когда пользователи Telegram совершают преступления, такие как распространение детской порнографии, торговля наркотиками, мошенничество или терроризм. Однако, это действие должно проводиться с соблюдением законодательства и только в рамках правового поля.

Применение деанонимизации должно сопровождаться защитой прав человека и неприкосновенностью личной жизни. Несанкционированная деанонимизация или слежка может нарушать законы о защите данных и приватности. Кроме того, важно помнить, что любые действия, связанные с деанонимизацией, должны проводиться в соответствии с международными стандартами и только для предотвращения или расследования преступлений.

Деанонимизация пользователя в Telegram или в любом другом сервисе подразумевает процесс установления личности конкретного человека, стоящего за анонимным аккаунтом [1]. Важно заметить, что деанонимизация пользователей без их согласия является нарушением их прав и в некоторых странах может быть незаконной.

Telegram весьма популярен благодаря своим функциям приватности и безопасности, но есть несколько способов, с помощью которых теоретически возможна деанонимизация (рисунок 1).

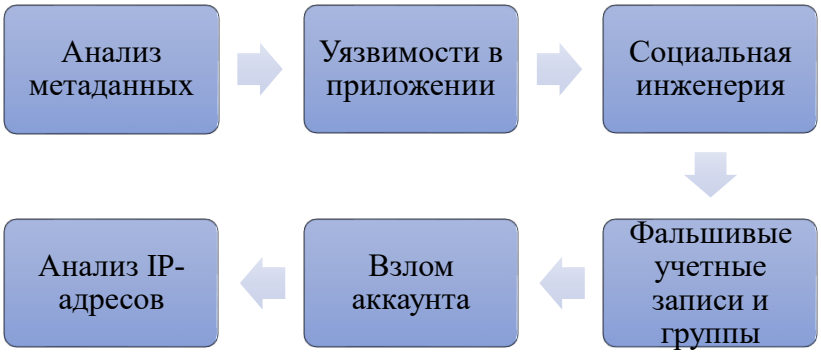

Рисунок 1. – Способы деанонизации в телеграмме

Анализ метаданных. Несмотря на то, что сообщения зашифрованы, метаданные (например, время отправки сообщения, частота общения с определенными контактами) могут быть проанализированы для создания социального графа или паттернов поведения пользователя.

Уязвимости в приложении. Любые недостатки в безопасности самого приложения Telegram могут быть использованы для деанонимизации пользователей. Однако Telegram регулярно обновляется, чтобы устранять подобные уязвимости.

Социальная инженерия. Применение тактик манипуляции для того, чтобы пользователь сам раскрыл свою личность или дал доступ к своему аккаунту.

Фальшивые учетные записи и группы. Создание поддельных аккаунтов и групп для сбора информации о пользователях.

Взлом аккаунта. Использование методов взлома, таких как фишинг, ключ-логгеры или эксплойты для получения доступа к аккаунту.

Анализ IP-адресов. Хотя IP-адреса пользователей Telegram защищены, при определенных условиях (например, при использовании Telegram через незащищенный прокси-сервер) IP-адрес может быть раскрыт.

Перечисленный список способов не является исчерпывающим.

На основе исследований программно-технического функционала Telegram, изучения и следственной практики в Институте Следственного комитета разработан примерный алгоритм действий по деанонимизации пользователей указанного мессенджера [2] (рисунок 2).

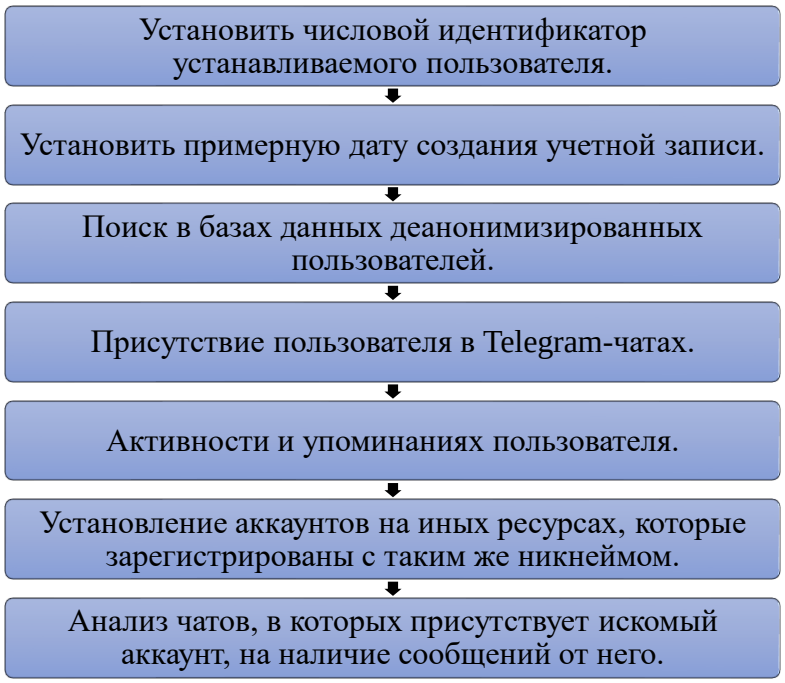

Рисунок 2. – Возможный алгоритм действий по деанонимизации пользователей Telegram

Данный алгоритм можно также добавить еще несколькими пунктами, например:

– использование законных запросов: правоохранительные органы могут использовать судебные ордеры, чтобы получить дополнительную информацию от Telegram или сторонних сервисов, которые могут хранить данные, связанные с подозреваемым;

– использование кибер-разведки: специализированные программные средства и техники кибер-разведки могут использоваться для сбора информации о цифровых следах пользователя в интернете;

– использование деанон-ботов: суть функционирования подобной ловушки заключается в пересылке устанавливаемому пользователю ссылки на бот, предлагающий некий функционал, который может заинтересовать искомое лицо, при запуске бот получает абонентский номер соответствующего пользователя (но следует отметить, что в клиентские приложения мессенджера заложен механизм обязательного предупреждения пользователя о сообщении боту его абонентского номера);

– ссылки-ловушки: при переходе по подобной ссылке, посланной под каким-либо предлогом устанавливаемому пользователю, инициатору становится известен IP-адрес и некоторые другие данные об используемом устройстве и программном обеспечении.

Резюмируя вышесказанное, стоит сказать, что деанонимизация пользователя осуществляется как киберпреступниками, так и лицами, рассекречивающими киберпреступников. Таким образом, деанонимизация как на носит вред, так и приносит пользу. Все зависит от того, какую цель преследует тот, кто прибегает к такому способу раскрытия информации о личности человека.

Хотелось бы также отметить, что Telegram известен своим сильным шифрованием и политикой конфиденциальности, так что деанонимизация пользователей без сотрудничества с самим Telegram или без серьезных оснований практически невозможна. Telegram продолжает оставаться одним из наиболее защищенных мессенджеров с точки зрения приватности пользователей.

Тем не менее, необходимо быть бдительными в отношении любых запросов личной информации и подозрительных сообщений. Чтобы избежать кибератак пользователям рекомендуется использовать двухфакторную аутентификацию, защищенные прокси или VPN.

Список литературы.

1. Шелудяков, Д.А. Исследование способов деанонимизации пользователей VPN-сервисов / Д.А. Шелудяков, С.А. Корчагин, Д.В. Сердечный // ООО Издательство «КУБиК». – г. Саратов., 2021. – 74 с.

2. Зарецкий, П.П. Деанонимизация пользователей мессенджера Telegram: обзор методов и инструментов / П.П. Зарецкий // Основные направления совершенствования системы национальной безопасности. – г. Минск., 2021. – С. 129-133.

3. Зулькарнеев, И. Р. Деанонимизация правонарушителей в сети Интернет / И. Р. Зулькарнеев, А. Е. Козлов, В. О. Нестор // Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. – 2019. – № 1-2. – С. 119-122.