Как выявить крота. Верифицируем участников проекта с помощью цифровых инструментов

Яков Пушной

https://te-st.org/2022/11/01/digital-verification/

Статья обновлена 28 декабря 2022

Новый участник гражданского движения быстро завоевал доверие. Он брался за любые поручения, постепенно перезнакомился с ключевыми фигурами. Потом стал администратором чата и получил доступ к общим ресурсам. А затем передал «правоохранителям» всю доступную ему информацию…

Можно ли избежать такого развития событий? В целом да. У верификации две главные задачи. Первая — убедиться, что человек действительно тот, за кого себя выдает. Вторая — удостовериться, что он подходит для вашего дела.

Какие данные собирать

Всякому организатору важно знать потенциальных участников его инициативы. Для сбора информации удобно использовать формы. Чаще используют Google Формы, но есть и альтернативы: например, Airtable и CryptPad.

Какую информацию запрашивать? Зависит от конкретной задачи и модели угроз. Например, если вы приглашаете людей на разовый вебинар, можно ограничиться минимумом информации. Если же вам нужно набрать исполнителей в проект, вероятно, вы захотите выяснить дополнительные подробности о потенциальных коллегах. Есть смысл опираться на

два основных принципа:

- данные должны собираться только для решения конкретных задач (а не «вдруг этот человек захочет участвовать еще в чем-нибудь»);
- не следует собирать избыточную информацию («узнаем больше — хуже не будет», «на всякий случай» или «ради общей картины»).

Вот пример одной из анкет для участников серии вебинаров по гражданско-правозащитной тематике. Звездочками помечены обязательные поля.

- Имя, фамилия (*).
- Организация, должность.
- Ваша профессиональная компетенция (перечисляются варианты: преподаватель, юрист-консультант, гражданский активист и т. д.) (*).
- Номер телефона для экстренной связи.
- Адрес электронной почты (*).
- Ник в Telegram (*).
- Страница в социальной сети.
- Откуда вы узнали о наших вебинарах (*).
- Почему вы хотите участвовать в наших вебинарах (*).
- Участвовали ли вы за последние 2 года в других подобных мероприятиях, если да, то каких?

Возможно, для некоторых ситуаций те или иные поля окажутся избыточными. Например, то, что организаторы активно используют Telegram внутри команды, вовсе не означает, что все потенциальные участники непременно должны установить Telegram (а значит, сообщить свои номера телефонов владельцам Telegram). Таким образом, обязательность поля «Ник в Telegram» может подталкивать людей к небезопасным для них решениям.

Как видно из примера, сбор данных напоминает весы. На одной чаше польза от информации. Скажем, ответ на вопрос об участии в других мероприятиях поможет оценить интересы человека, а при необходимости — навести о нем справки у организаторов этих встреч. На другой чаше весов — избыточность данных, вплоть до нежелательного нарушения границ частной жизни или потери у потенциального участника желания присоединиться к вам.

Очень важно четко определять рамки, кого вы хотите пригласить, а кого нет. Например, если вы ищете людей с определенным опытом работы или из конкретных регионов, вам следует об этом недвусмысленно сказать. Иначе возникает риск потратить ресурсы на верификацию кандидатов, которым вообще не место в вашем проекте. (Но выяснится это через несколько часов переговоров и анализа.)

Как быть с анонимностью? Вы можете оставить участника анонимным для остальных. В этом случае будет разумно сообщить ему об этом.

Юридическая ответственность

Данные, которые связаны с идентифицируемым человеком, считаются его персональными данными. В России обработку персональных данных регулирует Федеральный закон «О персональных данных» (152-ФЗ). По этому закону организатор становится оператором персональных данных. Операторы имеют обязанности и несут ответственность за нарушения порядка обработки данных. Штраф для физических лиц обычно несколько тысяч рублей, для

юридических — на порядок больше. Советуем прочитать нашу статью «Как собирать персональные данные и не нарушать закон».

В частности, вам придется создать правила обработки персональных данных: коротко и понятно объяснить, как вы планируете обрабатывать и использовать те данные, которые собираете. Вот пример:

Переданные вами данные будут использоваться только самими организаторами и только для целей обеспечения безопасности и коммуникации с вами. Информация не будет передаваться другим участникам. В течение 1 месяца после завершения мероприятия все персональные данные будут полностью удалены.

Человек, чьи данные вы собираете, должен дать свое недвусмысленное согласие на их обработку. Сделать это несложно. Например, добавить в форму поле «да/нет» и текст «Подтверждаю свое согласие с правилами обработки персональных данных» с гиперссылкой на созданные вами правила. Правила также должны описывать порядок отзыва этого согласия.

Использование собранных данных

Первую проверку можно сделать уже по собранным данным. Просто вычеркните тех, кто вам очевидно не подходит. Например, темнит и юлит с ответами, не может внятно сформулировать мотивацию к участию или вместо понятного ответа вписывает несколько бездушных штампов. Люди с адресом @mail.ru, которые хотят попасть на конференцию по безопасности, тоже вряд ли являются вашей целевой аудиторией.

Регистрационные данные можно использовать, чтобы получить рекомендации. В примере выше есть вопрос «Откуда вы узнали о наших вебинарах?». Ответ на него может помочь верификации или даже полностью решить вопрос. «Ваши вебинары мне посоветовал Андрей О.». Если вы знаете Андрея с хорошей стороны, замечательно. Можно связаться с ним непосредственно и попросить сказать пару слов о его отношениях с кандидатом.

- Да, я прекрасно знаю Бориса, действительно рассказывал ему о ваших вебинарах, я сам был на них в прошлом году. Борис замечательный человек и отважный активист. Я подумал, что ваши вебинары — именно то, что ему нужно в работе.
- Извините, не могу вспомнить никакого Бориса.

В первом случае верификацию можно считать пройденной. (Хотя конечно, если вам нужно больше информации для принятия решения, продолжайте.) Во втором случае поднимается красный флажок: похоже, кандидат попытался вас обмануть. Возможно, он рассчитывал, что проверять вы не станете.

Можно прямо спросить в регистрационной форме: «Кто может рекомендовать вас для участия?». Если таких персон (организаций) не одна, а две или еще больше, и это достойные, авторитетные люди, которых вы знаете, что ж, прекрасно…

OSINT: первые шаги

…Но возможно, регистрационных данных и рекомендаций окажется недостаточно.

Разведка по открытым источникам (Open-source intelligence, OSINT) — инструментарий из арсенала журналистов-расследователей. Эти средства во многом ориентируются на соцсети, но используют и открытые базы данных. Они зависимы от региона, где проживает тот, кого вы

проверяете. В нашей статье мы говорим преимущественно о россиянах. Но часть советов носит универсальный характер.

Сначала нужно позаботиться о собственной безопасности. Постарайтесь не использовать при переписке с кандидатом личные адреса электронной почты, аккаунты в мессенджерах и социальных сетях. Не звоните с личного телефона. Если вы собираетесь использовать инструментарий расследователя, обзаведитесь безопасным телефоном (можно виртуальным, например BlueStacks) и аккаунтами, которые никак не связаны с вами лично и используются только для мероприятий по проверке участников. Прочитайте статью Теплицы о том, как сделать смартфон анонимным.

Социальные сети

Страницы пользователя в соцсетях могут оказаться полезными для верификации. Убедитесь, что страница создана не вчера, у кандидата есть друзья, а публикации — соответствуют вашим представлениям о допустимом. Вряд ли суровый мужчина, заполнивший свой профиль селфи с разными видами автоматического оружия и бурно отмечающий милитаристские праздники, окажется эффективен в роли антивоенного активиста-волонтера. Фотографии, как опубликованные, так и те, на которых объект проверки отмечен друзьями, могут рассказать об увлечениях человека.

Бывает, что о человеке в соцсетях больше говорит его окружение, чем он сам. Поинтересуйтесь комментариями не только объекта, но и посетителей его страницы. Кто у него в друзьях? Кого объект чаще репостит, кого лайкает в комментах? В каких группах состоит? Могут оказаться полезны данные о семье. Если вдруг вы пригласите на вебинар «дочь мента», хорошо бы знать про это заранее.

Обратите внимание на статью Теплицы о том, сколько избыточной информации о себе люди выкладывают в соцсетях. То, что плохо для приватности, может быть полезно для верификации.

Инструменты расследователя

Будем считать, что для дальнейших действий вы используете безопасное устройство. Помните, пока вы собираете информацию о других — другие собирают информацию о вас. Некоторые сервисы поиска информации требуют оплаты. Такие платежи тоже должны быть безопасными. Например, можно использовать криптовалюту.

В некоторых странах обработка данных, полученных незаконным путем, — незаконна. А некоторые поисковые сервисы используют «сливы» персональных данных.

Представьте, что любая персонифицированная информация о человеке — имя, телефон, фото, адрес электронной почты или никнейм — это ниточка, за которую можно потянуть. Каждая ниточка дает еще одну ниточку, еще одну порцию информации. Какие-то из обнаруженных данных не будут иметь веса. Например, вы обнаружили, что у человека есть кот. Что с того? У негодяев тоже бывают домашние питомцы. Другие данные окажутся незначительными. Кот спасен с улицы. Возможно, его владелец добрый, эмпатичный человек. А может, кота спасла его мама, и это она добрый, эмпатичный человек. Насколько далеко яблоко упало от яблони, мы не знаем. Значит, есть смысл двигаться дальше. Постепенно портрет вашего объекта обретет более детальные черты.

В УК РФ есть статья 272 «Неправомерный доступ к компьютерной информации», аналогичные статьи есть в законодательстве и других стран. Поэтому мы ни в коем случае не призываем вас пробивать «клиента» по базе сервиса доставки еды и такси, хотя это может дать несколько постоянных адресов, и в том числе место службы. Да и распечатки звонков, хорошо

известные по нашумевшим расследованиям, хотя и позволяют определить не только круг близких людей, но и сослуживцев, — мы не рассматриваем как источник получения данных. Но если для вас детализированная проверка это вопрос физической безопасности участников и есть ресурсы на детальное расследование, лучше заняться этим до того, как этот человек сольет ваши базы электронных адресов.

Примеры поисковых инструментов

https://search4faces.com/ — поиск по публичным фотографиям во ВКонтакте, Одноклассниках, TikTok, ClubHouse. Попробуйте использовать несколько фотографий при поиске.

Хотя https://findclone.ru/ и обещает найти «вашего цифрового двойника», но это тот же поиск любого человека по фотографии во ВКонтакте. Впрочем, результат может отличаться от search4faces.

https://220vk.com/ позволяет обнаружить скрытых друзей. Кого пользователь комментирует, кому ставит лайки и так далее. Можно также установить родственные и деловые связи.

Поисковые Telegram-боты

Много информации можно найти с помощью ботов. Но при этом вы вынуждены использовать Telegram. Значит, Telegram ID становится известен боту. Сервис бота можно сопоставить с тем, в каких каналах вы зарегистрированы с вашими контактами. Ваш запрос к боту для кого-то другого может стать той ниточкой, которая раскроет информацию о вас. Поэтому повторим свой совет: создайте анонимный аккаунт Telegram, зарегистрированный на анонимную SIM-карту на безопасном устройстве.

@QuickOSINT_bot осуществляет поиск в официальных государственных и общедоступных коммерческих источников, базах данных такси, банков, страховых компаний и т.д.

@helper_inform_bot имеет примерно те же источники данных. Но, как и в случае поиска по фото, этот бот использует другие алгоритмы. При поиске данных по конкретной персоне отличия могут быть существенными.

himera-search.info пригодится, если ничто из перечисленного не помогло. Доступен в форматах онлайн-сервиса и Telegram-бота.

Поиск по данным Getcontact

Мы не станем рекомендовать приложение Getcontact для установки. Вряд ли вы хотите поделиться базой контактов с посторонними людьми. Но сам инструмент может быть полезен для верификации. Например, вы можете узнать, что энергичный организатор мероприятий Саша у кого-нибудь записан как «Александр Центр Э». А солидная Мария Викторовна (23 года работы главным бухгалтером), предложившая свою помощь с финансовой отчетностью, известна как «Гадалка Марфа».

При поиске не забывайте о разных словоформах и написании слов, возможных ошибках, об использовании повторяющихся частей в разных никнеймах и аккаунтах.

Что в итоге?

В обработке результатов вам помогут старые добрые таблицы. Можно использовать Таблицы Google или, например, Cryptpad.

Разбейте проверку на этапы и каждый этап фиксируйте в таблице. Для оценки сформулируйте несколько параметров. Например: полнота предоставленных данных, результат проверки

профилей в социальных сетях, найденные профили по результатам поиска и т.п.

Некоторые параметры — критические. Если предоставлен фейковый аккаунт социальной сети, то дальнейшие и рассматривать нет никакого смысла. Другие параметры, такие как полнота данных или мотивация, можно оценивать по шкале от 0 до 10 и по сумме параметров принимать решение о продолжении проверки.

Есть и другие, нетехнические способы верифицировать будущих участников ваших проектов. К примеру, личный контакт. Если вам позволяют ресурсы, можно провести видеочат с кандидатом и задать вопросы. Иногда такой чат, пусть даже совсем короткий, важен для верной идентификации кандидата. Например, если у вас появились сомнения, тот ли человек с вами на связи, за кого он себя выдает. Убедитесь, что фото в профиле соответствует оригиналу. Задайте собеседнику вопросы, поговорите, например, о том, каким он видит свой вклад в общую работу.

Методы проверки многогранны и неидеальны, и даже безупречный человек может резко изменить свои взгляды или быть завербованным. Проверки не отменяют необходимость в мерах безопасности, разработке политик безопасности, тренингах. Тем не менее входные фильтры, описанные в этой статье, помогают снизить риски.