Предотвращение раскрытия данных и перепись населения

Выбор тем при международных переписях населения[1]

Sam Dupre, Lindsay Spell, Paul Jung

Опубликовано в марте 2022 г.

ВВЕДЕНИЕ

Геокодированные данные становятся доступными со все более высоким разрешением, а возможности злоумышленников по привязке геокодированных данных к конкретными людям или группами продолжают расти. Количество идентифицирующих переменных, необходимых для утечки данных, резко сокращается, когда точно известно географическое местоположение, особенно там, где плотность населения низкая. Разработка источников геокодированных данных создает новые проблемы в связи с нарушением конфиденциальности, так как традиционные механизмы предотвращения раскрытия сведений могут игнорировать пространственные характеристики (Buron and Fontaine, 2018).

Хотя географические характеристики технически являются всего лишь еще одной переменной, есть определенные аспекты, которые делают их достойными дальнейшего рассмотрения.

Национальные статистические управления (NSO, в соответствии с английским акронимом) в настоящее время находятся в сложном положении, поскольку им приходится распространять данные переписи среди пользователей, сохраняя при этом пространственные отношения и принимая во внимание особенности пространственных данных при контроле за раскрытием статистических сведений. Важно отметить, что чувствительность переменных и населения сильно различается в зависимости от национального контекста; не существует универсального подхода к предотвращению раскрытия информации.

В данной технической записке обсуждаются ключевые концепции предотвращения раскрытия геопространственных данных и содержится обзор процесса с примером реализации. Данная записка составлена на основе материалов, представленных в документе «Предотвращение раскрытия информации и перепись населения» (U.S. Census Bureau, 2020). Краткое изложение этого руководства приведено в поле 1.

[1] Настоящая техническая записка является частью серии «Избранные темы международных переписей населения» (STIC, в соответствии с английским акронимом), в которой рассматриваются вопросы, представляющие интерес для международного статистического сообщества. Бюро переписи населения США помогает странам совершенствовать национальные системы статистики, содействуя устойчивому расширению статистических компетенций. Любые выраженные мнения отражают точку зрения автора(-ов) и не обязательно совпадают с позицией Бюро переписи населения США.

Поле 1.

Общие сведения о предотвращении раскрытия информации

Законодательные требования

Хотя законодательные требования по защите конфиденциальности данных респондентов варьируются от страны к стране, эти меры имеют решающее значение для поддержания общественного доверия и готовности участвовать в переписях и опросах.

Действия по предотвращению

1. Удаление личную информацию (PII, в соответствии с английским акронимом).
2. Определение конфиденциальных записей, ячеек и категорий.
3. Устранение рисков.
4. Проверка результатов.
5. Внутренние исследования атак.

Типы

- Раскрытие личности — распространяемый набор данных напрямую связан с личностью респондента.
- Раскрытие атрибутов — распространяемый набор данных напрямую связан с другими характеристиками респондента.
- Раскрытие путем умозаключений — распространяемый набор данных может использоваться для того, чтобы сделать выводы о респонденте при помощи статистических методов работы с данными.

U.S. Department of Commerce
U.S. CENSUS BUREAU
census.gov

United States Agency for International Development
www.usaid.gov

United Nations Population Fund
www.unfpa.org

КЛЮЧЕВЫЕ ПОНЯТИЯ

Проблемы оценки небольших областей

Многие NSO выпускают наборы данных о населении небольших областей, чтобы точно определить пространственное распределение населения, вплоть до единицы сбора данных/квартала переписи. Однако публикация данных с высоким разрешением может увеличить риск раскрытия личности. Поскольку данные по небольшим областям, вероятно, будут иметь более низкие значения ячеек, существует более высокая вероятность обратного геокодирования (см. поле 2) с последующим раскрытием личности с использованием точных пространственных атрибутов и характеристик распределения населения в пределах области.

Вложенные иерархии

Довольно легко оценить риск дифференцирующей атаки, если используются вложенные данные (см. поле 2). С невложенными данными связаны более сложные ситуации.

Если наборы геопространственных данных построены с использованием вложенных иерархий, раскрытие идентичности можно предотвратить путем подавления данных в областях с низкими значениями. Поскольку между областями одного уровня нет перекрытий, дифференцирующая атака вряд ли будет успешной.

Однако при наличии невложенных данных имеет место высокий риск дифференцирующих атак и раскрытия личности. Например, если невложенная зона помещается в пределах области переписи, дифференцирование невложенной зоны относительно окружающей области переписи позволяет найти некоторое количество домохозяйств, которые находятся в дифференцированной зоне и могут быть идентифицированы как местонахождение респондентов. Если дифференцированная зона имеет атрибут с низким значением и редкое распределение населения, существует высокая вероятность того, что местонахождение и личности респондентов могут быть раскрыты. Подобная дифференцирующая атака может также произойти, когда невложенная зона или ячейка с координатной сеткой помещаются между двумя областями переписи.

Микроданные и агрегированные данные

NSO публикуют данные двух типов: микроданные и агрегированные данные (U.S. Census Bureau, 2020). Существует несколько способов, при помощи которых каждая форма может быть снабжена пространственной информацией. Дополнительные сведения о процедурах, связанных с каждой формой, рассматриваются далее в этом документе.

Микроданные предназначены для отдельных респондентов. Они обезличиваются и публикуются с пространственным атрибутом, указывающим местонахождение отдельных респондентов. Когда микроданные публикуются вместе с координатами, геомаскирование (рассматривается далее в этом документе) обезличивает их точное местоположение и предотвращает раскрытие данных путем внесения в координаты искусственных ошибок.

Агрегированные данные получаются путем пространственного обобщения с использованием административных или статистических единиц (например, районов или ячеек с координатной сеткой) в целях предоставления информации о местоположении на основе области (рисунок 1). Поскольку агрегированные данные с пространственными атрибутами дают приблизительную информацию о местоположении респондентов, их конфиденциальность может быть защищена путем подавления данных в областях с низкими значениями.

Поле 1.— Продолжение

Принципы

- Публиковать образцы из более крупных/плотно населенный районов.
- Уменьшать вариативность ниже порогового значения.
- Скрывать данные, в которых видны уникальные случаи.
- По возможности сохранять исходные отношения/структуру данных.

Источник: U.S. Census Bureau, 2020.

Поле 2.

Некоторые типы атак

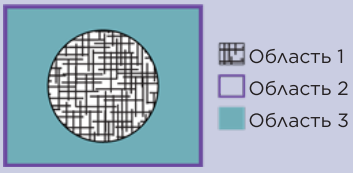
Обратное геокодирование

Геокодирование — это процесс преобразования текстового адреса или названия места в географические координаты для определения точного местоположения данных исследования.

Обратное геокодирование происходит, когда определяется почтовый адрес места, опубликованного в бумажном или цифровом формате. В таких случаях адреса улиц могут стать мощным средством для связывания данных по этим координатам с конкретными идентифицируемыми сведениями из других источников. Местонахождение респондентов может быть установлено путем логических заключений и подвергнуто обратному геокодированию, если в области переписи есть ячейки с низкими значениями.

Дифференцирующие атаки

Такие атаки происходят, когда данные, опубликованные на разных географических уровнях, могут быть объединены в целях реконструкции данных на более низком уровне или определения места наблюдения. Например, на приведенном ниже рисунке область 1 является подмножеством области 2. Поэтому можно создать таблицу со статистикой по области 3, которая может не соответствовать стандартам конфиденциальности.



Если географическая дифференциация позволяет создать географию с меньшим числом респондентов, чем минимальный порог, происходит утечка данных.

Источник: U.S. Census Bureau, 2021.

Геомаскирование

Геомаскирование — это геопространственный процесс, повышающий защиту конфиденциальности за счет систематического добавления синтетического шума к координатам адресов респондентов. Имеется множество методов геомаскирования. В качестве примера можно привести два распространенных метода: метод пончика и пространственное сглаживание (Buron & Fontaine, 2018). В простейшей версии метод пончика заключается в том, что все геокодированные адреса смещаются относительно истинной точки в случайном направлении на расстояние, которое лежит в заданном диапазоне значений. Пространственное сглаживание заключается в смешивании данных из локальных, пространственно смежных областей, в результате чего образуются средневзвешенные значения для участков вокруг точки (пример использования данного метода и влияющих на данные параметров показан на рисунке 2). Применение пространственного сглаживания может быть таким же простым, как формирование тепловой карты вместо картограммы для сглаживания соседних областей при визуализации. Более подробно геомаскирование описано далее в этом документе.

Основные моменты концепции

1. При геомаскировании устанавливаются географические или числовые ограничения, которые позволяют свести к минимуму искажение пространственных атрибутов микроданных или усилить защиту конфиденциальности. Нежилые районы (например, водоемы, парки и зеленые зоны), можно отфильтровать и гарантировать, что точки с геомаскированием там не появятся. Ограничение также позволяет не допустить чрезмерного смещения геомаскирования в пределах единицы переписи, в которой находится исходная точка. Благодаря этому удается максимально сохранить пространственные атрибуты респондентов. Поскольку в областях с низкой плотностью населения респонденты подвержены более высокому риску раскрытия личности, степень смещения может быть установлена обратно пропорционально плотности населения. Местоположение может быть идеальным «ключом», который с высокой степенью достоверности связывает общедоступные и анонимные несвязанные наборы данных.
2. Инструменты, подобные Google Earth, и ресурсы, предоставляющие открытый доступ к данным, позволяют людям получать данные о местоположении, а затем тем или иным способом отслеживать местоположение конкретных респондентов.
3. Имеющиеся в пространственных данных несоответствия и указания на конкретные местоположения могут быть причиной для утечки данных.
4. Невложенные области могут быть критическим фактором риска для дифференцирующих атак.

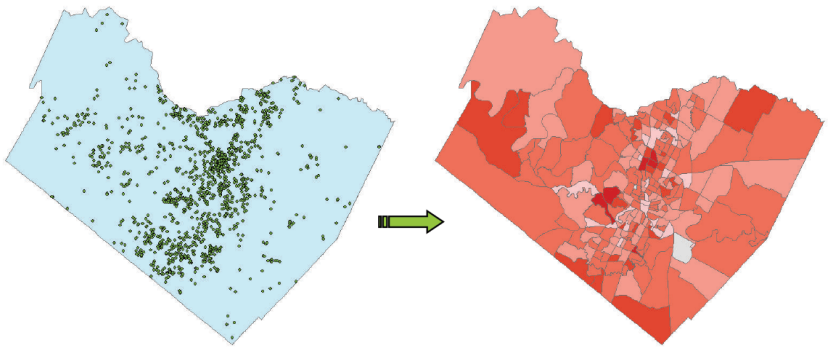
ОБЗОР ПРОЦЕССА

Планирование публикации

Как можно раньше в процессе переписи NSO должно начать планировать следующие три аспекта публикации географических данных:

- Конкретные географические районы, по которым будут опубликованы данные.
- Географические уровни детализации (например, провинция, район или квартал), которые необходимо опубликовать.
- Форма(ы) публикуемых данных (микроданные, агрегированные векторные или растровые данные).

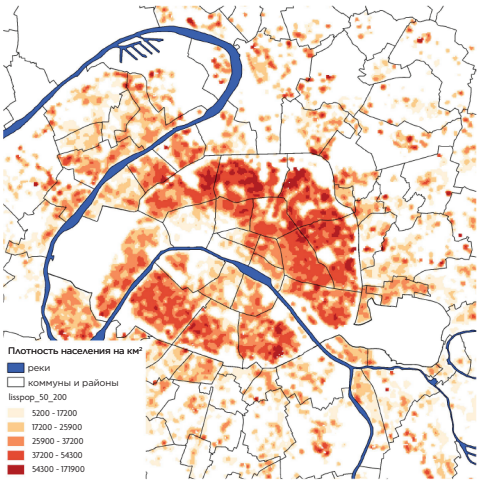
Рисунок 1.
Объединение пространственных данных из отдельных точек



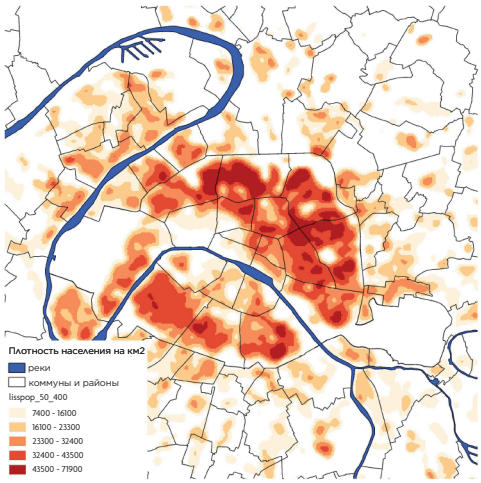
Источник: Zandenbergen, 2014.

Рисунок 2.

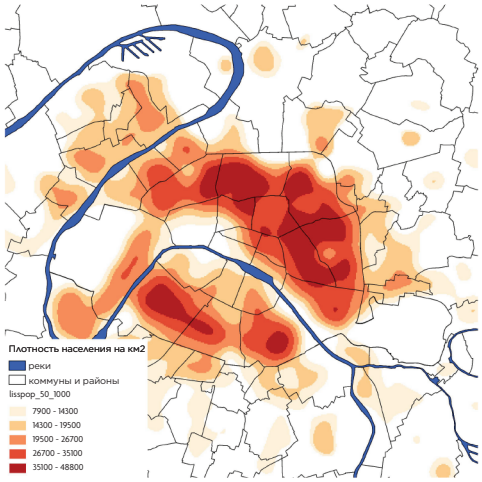
Три радиуса для сглаживания плотности населения в Париже и его пригородах



(a) Радиус 200 м



(b) Радиус 400 м



(c) Радиус 1000 м

Источник: Genebes et al., 2018.

Эти решения представляют собой первые шаги, которые необходимо сделать, так как они определяют методы сохранения конфиденциальности, которые необходимо применить. В частности, может оказаться, что NSO будет должно опубликовать меньше данных, чем изначально планировалось.

Оценка рисков раскрытия информации

Сначала NSO необходимо проанализировать планы публикации, включая прошлые выпуски, чтобы установить, не существуют ли одни и те же (или перекрывающиеся) данные в нескольких формах. Публикация геомаскированных точечных данных для области, для которой ранее уже публиковался набор пространственных агрегированных векторных данных, снижает уровень защиты конфиденциальности как для старого, так и для нового набора. Если это так, область перекрытия точечных и агрегированных векторных данных должна быть помечена как «подверженная риску».

Затем NSO необходимо проверить все результаты обработки данных на наличие перекрытий между невложенными географическими регионами. Домохозяйства в перекрывающихся областях должны быть помечены как «подверженные риску».

После этого NSO необходимо воспользоваться методами, которые изложены в документе «Предотвращение раскрытия данных и перепись населения» (U.S. Census Bureau, 2020), для блокировки областей, в которых:

- Наличие ячеек, соответствующих небольшому подмножеству.
- Наличие ненулевых значений подсчета уязвимых групп.
- Различные подмножества результатов включают одну и ту же совокупность (совокупности) населения.
- Лица, находящиеся в домохозяйстве, отмечаются в качестве находящихся в группе риска.
- В ответах для любой переменной имеются выпадающие значения.

Устранение риска

После того, как наборы данных, домохозяйства и отдельные лица, находящиеся в группе риска, отмечены флажками, могут быть приняты меры для снижения риска раскрытия информации. В данном документе мы рассматриваем материалы, относящиеся к проблемам геоконфиденциальности; альтернативные методы, которые не зависят от пространственного положения, включая контроль доступа через анклавы данных с ограниченным доступом, обсуждаются в документе «Предотвращение раскрытия данных и перепись населения» (U.S. Census Bureau, 2020).

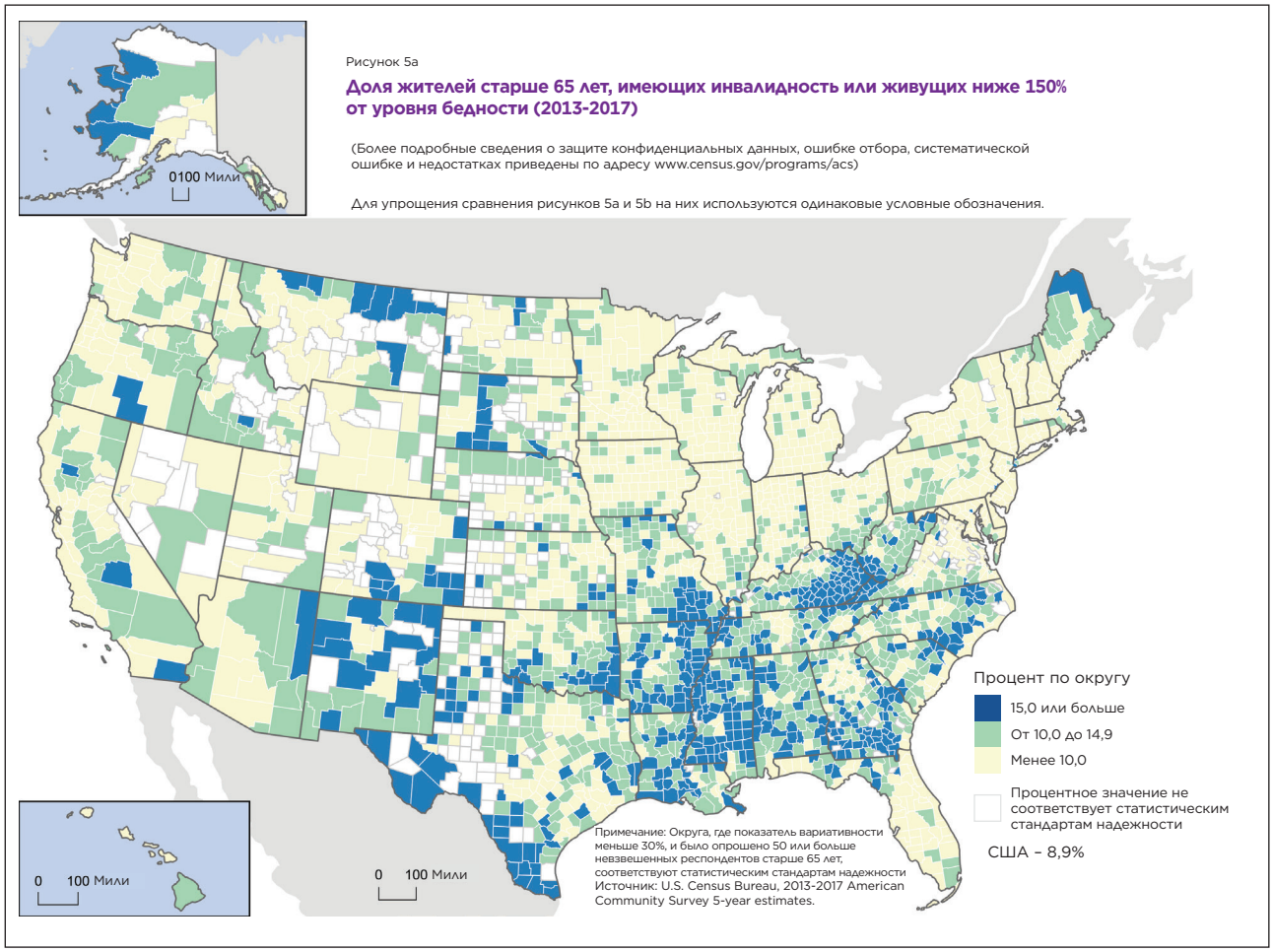
Важно отметить, что ни один набор данных не должен публиковаться более одного раза с применением различных средств защиты конфиденциальности. Два выпуска данных из одного и того же набора данных с использованием разных методов могут быть использованы для раскрытия сведений о респондентах.

Подавление

Самый простой способ защитить данные на уровне отдельных лиц или домохозяйств — не публиковать их. В таких случаях польза от публикации должна перевешивать любой риск разглашения. Подавление позволяет защитить конфиденциальность респондентов путем замены ячеек с атрибутами в агрегированных таблицах или на объектах карты маркером «нет данных». Такая замена производится, если значение атрибута не превышает порогового значения. Такой процесс предотвращает потенциальные дифференцирующие атаки, во время которых области с имеющими низкие значения ячейками сопоставляются с другими наборами данных. На рисунке 3 приведен пример, когда многоугольники, подверженные риску, были заменены пустыми многоугольниками, указывающими на то, что «процент не соответствует статистическим стандартам надежности». Замена производилась, когда число респондентов и статистические показатели указывали на то, что возможно раскрытие конфиденциальной информации, а сами данные ненадежны для конкретного набора данных. NSO могут подавлять целые наборы данных, опускать некоторые неагрегированные данные

Рисунок 3.

Пример продукта бюро переписей населения, в который не входят округа с высоким уровнем риска



Источник: U.S. Census Bureau, <www.census.gov/content/dam/Census/library/visualizations/time-series/demo/older-population/Figure%205%20Population%20Aged%2065%20and%20Over%20with%20a%20Disability%20in%20Poverty.pdf>, 2019.

(подавляя менее полезные для общественности сведения) или некоторые ячейки.

При подавлении данных NSO следует учитывать как первичное, так и вторичное подавление. Первичное подавление заключается в пропуске ячеек или точек, в которых ранее были отмечены респонденты. Последующее вторичное подавление заключается в подавлении данных, публикация которых позволит деанонимизировать данные в ячейках первичного подавления. NSO необходимо сравнить данные, опубликованные на разных уровнях вложенной географической иерархии, чтобы выявить (возможно, в других наборах данных) ячейки, которые требуют вторичного подавления. Более подробные сведения о первичном и вторичном подавлении приведены в документе «Предотвращение раскрытия данных и перепись населения» (U.S. Census Bureau, 2020).

Геомаскирование

Как описано выше, геомаскирование может использоваться для статистического добавления синтетического шума либо к координатам адресов респондентов, либо к атрибутивным данным для домохозяйств или районов. Когда микроданные публикуются с координатами респондентов, геомаскирование может предотвратить раскрытие личности путем обратного геокодирования, дифференцирующей атаки или их сочетания. Геомаскированные координаты смещаются на достаточное расстояние от исходных точек, а затем используются для замены исходных координат.

Выбор параметров и методов геомаскирования должен осуществляться с учетом рассматриваемого местоположения. Например, алгоритм, который случайным образом смещает точки в пределах 50–150 метров, может быть эффективен в плотном городском районе, но вряд ли обеспечит защиту конфиденциальности в сельской местности.

Пространственное агрегирование

Пространственное агрегирование в укрупненных единицах переписи большой площади снижает риск раскрытия личности, когда агрегированный набор данных в единице переписи меньшей площади подвержен риску раскрытия. Агрегированные данные повышают конфиденциальность респондентов за счет преобразования их местонахождения из набора точек в пространственную фигуру. Однако, если на месте проведения переписи имеет место низкая плотность населения или находится небольшое относительно общей численности населения количество респондентов, их личности можно легко установить и по основе агрегированным данным. В таких случаях NSO может агрегировать более крупную пространственную единицу с достаточно большим количеством населения или респондентов. Пороговые значения для агрегирования определяются с учетом чувствительности данных и местного распределения населения.

Временное разрешение

Когда это возможно, NSO могут установить временное разрешение публикуемых данных. Если злоумышленник знает местонахождение респондента в определенное время, он может очень легко определить место его работы, жительства и отдыха. Во поле 3 приведен пример того, как городские власти Нью-Йорка скорректировали временное разрешение при реагировании на COVID-19.

Поле 3.

Тематическое исследование: данные о состоянии здоровья с географической привязкой и пандемия COVID-19

Пандемия COVID-19 привлекла внимание к наблюдению за местоположением, карантину, социальному дистанцированию и ограничению мобильности. Органы общественного здравоохранения отслеживают контакты людей, чтобы замедлить распространение COVID-19 в местных сообществах. Для точного отслеживания контактов NSO и органы общественного здравоохранения собирают и объединяют различные наборы данных с географической привязкой, включая местонахождение лиц с подтвержденным положительным диагнозом и записи траекторий их движения. Источниками сведений являются опросы, данные из социальных сетей и многое другое. Однако объединенные данные с географической привязкой имеют высокий риск раскрытия личности, что вызывает опасения по поводу конфиденциальности.

Когда NSO и органы общественного здравоохранения используют закрытые медицинские данные с географической привязкой, они применяют различные методы для обеспечения безопасности данных и защиты конфиденциальности. Например, органы здравоохранения Южной Кореи следуют протоколу конфиденциальности, согласно которому при отслеживании контактов все данные полностью анонимизируются, шифруются и объединяются в грубых пространственных единицах.

Из-за конфиденциальности медицинской информации публикация подтвержденных случаев осуществляется с особой осторожностью. Особое внимание уделяется пространственному разрешению. Нью-Йорк публикует наборы данных о подтвержденных или вероятных случаях заражения, случаях госпитализации и подтвержденных случаях смерти. Эти наборы объединяются на уровне почтовых индексов. Записи передаются ежедневно с трехдневной задержкой, поэтому раскрытие личности может быть эффективно предотвращено.

Источник: Smith, 2020; NYC Health, 2021; World Bank, 2021.

Проверка результатов

При проверке эффективности механизмов защиты данных NSO должно задать себе три вопроса.

1. Достаточно ли были анонимизированы данные?
2. Сведены ли к минимуму любые искажения пространственных отношений, вносимые при анонимизации?
3. Достаточно ли информативны опубликованные метаданные при условии, что эффективность анонимизации не снижается?

Эффективность механизмов защиты данных. Чтобы ответить на первый вопрос – достаточно ли были анонимизированы данные? — можно использовать пространственную k-анонимность, то есть идею о том, что субъект не может быть идентифицирован среди k-1 других субъектов. Пространственная k-анонимность аналогична непространственной k-анонимности, однако вместо связывания записей в базе данных в качестве механизма угрозы раскрытия используется обратное геокодирование. Даже когда в результате геомаскирования местоположение смещается на значительное расстояние от исходной точки, это не гарантирует исключительную конфиденциальность. Если в этом районе имеется относительно небольшое количество возможных мест проживания, одно из них может быть повторно идентифицировано как первоначальное местонахождение респондента, и конфиденциальность будет нарушена. Это может часто происходить в малонаселенных районах, где рядом с геомаскированными и исходными местоположениями находится всего несколько жилых районов. Важно проверить, обеспечивает ли геомаскирование достаточно большое количество жилых местоположений, что затрудняет повторную идентификацию исходного местоположения. Чтобы гарантировать требуемый NSO уровень конфиденциальности, перед публикацией микроданных можно установить минимальное пороговое значение количества расположенных рядом мест проживания.

Сведены ли к минимуму любые искажения пространственных отношений? Чтобы ответить на второй вопрос — сведены ли к минимуму любые искажения пространственных отношений, вносимые при анонимизации? — NSO необходимо рассмотреть и установить компромисс между пространственным искажением и риском для конфиденциальности. Если в процессе геомаскирования установить более высокий уровень конфиденциальности (за счет увеличения расстояния, на которое смещаются координаты, или минимально допустимого расстояния до ближайших населенных пунктов, находящихся рядом с маскируемыми локациями), разница между геомаскируемой и исходной локациями увеличивается, а качество данных пространственных атрибутов снижается. Такое искажение может привести к значительной систематической ошибке в аналитических результатах, основанных на этих данных. К сожалению, для явной оценки избыточности требуются как анонимные, так и неанонимные наборы данных, поэтому сторонние исследователи не могут выполнить такую оценку без помощи NSO. Тем не менее, NSO может сотрудничать с исследователями и выполнять такую оценку при наличии конкретных запросов. Вероятно при этом будет иметь место процесс согласования, а NSO возьмет за проделанную работу некоторую сумму денег.

Опасны ли метаданные? Чтобы ответить на третий вопрос — достаточно ли информативны опубликованные метаданные при условии, что эффективность анонимизации не снижается? — NSO должно публиковать как можно меньше метаданных о процессах геомаскирования и агрегирования, которые используются при публикации. Например, если злоумышленник узнает, что при геомаскировании использовалось нормальное, а не случайное распределение, он может более точно нацелить атаку, исходя из предположения, что истинное местоположение точки, вероятно, находится в пределах определенного диапазона. Публикация описаний методов, параметров маски и применяемых статистических условиях существенно снижает эффективность этих мер (Kounadi and Leitner, 2014).

ЗАКЛЮЧЕНИЕ

Содержащие пространственные сведения данные очень важны для эффективного государственного управления как во время кризиса (см. поле 3), так и в обычных условиях. По мере распространения инициатив по открытым данным и совершенствования технологий географической информационной системы (GIS, в соответствии с английским акронимом) информация с пространственными данными становится все более доступной и точной. При этом риск утечки конфиденциальных географических данных за последние десятилетия резко возрос. NSO находятся в выгодном положении, поскольку в них тесно сотрудничают сильные статистики, географы и социологи. Учитывая надлежащее внимание к конкретным рискам и возможностям, которые открывают меры геоконфиденциальности, NSO имеют хорошие возможности для продолжения публикации данных для общественного блага. Однако при этом необходимо поддерживать достаточную степень доверия респондентов, применяя надежные меры защиты геоконфиденциальности.

ЛИТЕРАТУРА

Antal, L., T. Enderle, and S. Giessing, «Harmonised Protection of Census Data in the ESS: Statistical Disclosure Control Methods for Harmonised Protection of Census Data,» Eurostat Centre of Excellence on Statistical Disclosure Control, The Hague, 2017.

Buron, M. L. and M. Fontaine, «14. Confidentiality of Spatial Data,» in Loonis, V. and M. de Bellefon, *Handbook of Spatial Analysis: Theory and application with R*, Insee Méthodes No. 131, Eurostat, 2018.

Camenisch, J., S. Fischer-Hubner, and M. Hansen (eds), «Privacy and Identity Management for the Future Internet in the Age of Globalisation (IFIP Advances in Information and Communication Technology),» Springer, 2016.

Genebes, L., Renaud, A., and F. Sémécurbe, «8. Spatial Smoothing,» in Loonis, V. and M. de Bellefon, *Handbook of Spatial Analysis: Theory and application with R*, Insee Méthodes No. 131, Eurostat, 2018.

Gutmann, M., K. Witkowski, C. Colyer, J. McFarland O'Rourke, and J. McNalley, "Providing Spatial Data for Secondary Analysis: Issues and current practices related to confidentiality," *Population Research and Policy Review*, 27(6): pp. 639–665, 2009.

Haley, D. F., S. A. Matthews, H. L. F. Cooper, R. Haardörfer, A. A. Adimora, G. M. Wingood, and M. R. Kramer, "Confidentiality Considerations for Use of Social-Spatial Data on the Social Determinants of Health: Sexual and Reproductive Health Case Study," *Social Science and Medicine*, 166: pp. 49–56, 2016.

Kounadi, O. and M. Leitner, "Why Does Geoprivacy Matter? The Scientific Publication of Confidential Data Presented on Maps," *Journal of Empirical Research on Human Research Ethics*, 9(4), pp. 34–45, 2014.

Laaribi, A. and L. Peters, "GIS and the 2020 Census," Esri Press, Redlands, CA, 2019.

Lauger, A., B. Wisniewski, and L. McKenna, "Disclosure Avoidance Techniques at the U.S. Census Bureau: Current Practices and Research, Research Report Series (Disclosure Avoidance #2014-02)," Center for Disclosure Avoidance Research, U.S. Census Bureau, Washington, DC, 2014.

McKenna, L. and M. Haubach, "Legacy Techniques and Current Research in Disclosure Avoidance at the U.S. Census Bureau," Research and Methodology Directorate, U.S. Census Bureau, Washington, DC, 2019.

NYC Health, COVID-19: Latest Data - NYC Health, <https://www1.nyc.gov/site/doh/covid/covid-19-data.page#epicurve>, accessed on March 11, 2021.

Pascale, J., D. K. Willimack, N. Bates, J. F. Lineback, and P. C. Beatty, "Issue Paper on Disclosure Review for Information Products with Qualitative Research Findings," Research and Methodology Directorate, U.S. Census Bureau, Washington, DC, 2020.

Smith, C. D. and J. Mennis, "Incorporating Geographic Information Science and Technology in Response to the COVID-19 Pandemic," Preventing Chronic Disease, 17, E58, 2020.

United Nations Statistics Division, "Principles and Recommendations for Population and Housing Censuses, Revision 3," United Nations Publications, New York, NY, 2015.

United States Census Bureau, "Disclosure Avoidance and the Census," Select Topics in International Censuses, <www.census.gov/content/dam/Census/library/working-papers/2020/demo/disclosure_avoidance _and_the_census_brief.pdf>, 2020.

United States Census Bureau, "Figure 5: Population Aged 65 and Over With a Disability in Poverty, Select Maps on the Population 65 and Older in the United States by County: 2013–2017," <www.census.gov/content/dam/Census/library/visualizations/time-series/demo/older-population/Figure%205%20Population%20Aged%2065%20and%20Over%20with%20a%20Disability%20in%20Poverty.pdf>, 2019.

World Bank, "The Role of Geospatial Information in Confronting COVID-19 – Learning From Korea," <https://blogs.worldbank.org/eastasiapacific/role-geospatial-information-confronting-covid-19-learning-korea>, accessed on March 11, 2021.

Zandenbergen, P. A., "Ensuring Confidentiality of Geocoded Health Data: Assessing Geographic Masking Strategies for Individual-Level Data," *Advances in Medicine*, 2014.

Zayatz, L., "Disclosure Avoidance Practices and Research at the U.S. Census Bureau: An Update," Research Report Series (Statistics #2005-06), Statistical Research Division, U.S. Census Bureau, Washington, DC, 2005.

United States® Census Bureau

USAID FROM THE AMERICAN PEOPLE

UNFPA

Серия «Избранные темы международных переписей населения» публикуется в рамках Международных программ Отдела народонаселения Бюро переписи населения США. Агентство США по международному развитию финансирует подготовку серии STIC и двустороннюю поддержку статистических организаций, которые предоставляют информацию авторам. Фонд ООН в области народонаселения участвует в подготовке содержания и обнародовании документов STIC, способствуя их распространению среди более широкой аудитории.