МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

Институт компьютерных наук и кибербезопасности

Высшая школа технологий искусственного интеллекта

Отчёт по дисциплине «Образовательный форсайт»

Анонимизация данных

Студент: _____ Салимли Айзек Мухтар Оглы

Преподаватель: _____ Курочкин Михаил Александрович

«____»_____ 20__ г.

Санкт-Петербург, 2025

Содержание

Введение

В рамках модуля мобильности был выбран курс «Анонимизация данных», так как направление данного курса, нужно для защиты персональных данных. Автором курса, является ведущий специалист в области анонимизации данных - д.т.н., доцент Института компьютерных наук и кибербезопасности - Полтавцева Мария Анатольевна. Курс включает в себя 6 содержательных тем. Все материалы курса доступны с момента открытия курса: видеолекции, кратко раскрывающие содержание каждой темы, презентации и конспекты, с которыми в дальнейшем можно ознакомиться в любое удобное время. Все темы включают практические занятия и самостоятельные работы. В материалах курса подготовлены методические рекомендации к выполнению заданий и примеры решения типовых заданий.

1 Постановка задачи

В рамках курса «Образовательный форсайт», было необходимо пройти выбранный по желанию онлайн курс «Анонимизация данных» на портале «Открытое образование» (https://openedu.ru/). Онлайн-курс предполагает успешное освоение предлагаемых десяти лекций, написание контрольных заданий по лекциям и итогового теста. Цель изучения дисциплины «Анонимизация данных» заключается в освоении базовых принципов и методов анонимизации данных.

2 Аннотация курса и разделов

В настоящее время анонимизация данных является критически важным направлением в области информационной безопасности и защиты персональных данных. Этот курс представляет собой комплексное изучение современных методов и технологий обеспечения конфиденциальности информации в условиях цифровой трансформации. Анонимизация данных формирует основу для безопасной работы с персональной информацией, позволяя использовать данные для анализа и исследований, сохраняя при этом приватность пользователей.

Технологии анонимизации находят широкое применение в различных сферах деятельности, включая здравоохранение, финансы, государственное управление и бизнес-аналитику. Они предоставляют возможность работать с большими объемами данных, соблюдая требования законодательства о защите персональных данных и обеспечивая баланс между доступностью информации и её конфиденциальностью. Это делает знания в области анонимизации данных особенно ценными в современном мире, где вопросы защиты информации становятся все более актуальными.

3 Теоретическая часть курса

3.1 Базовые понятия

- **Анонимизация (персональных) данных** - действия, направленные на сохранение конфиденциальности данных путем защиты от атак идентификации.
- **Атака логического вывода (inference attack)** – атаки нарушения конфиденциальности данных, которые проводятся без нарушения политики безопасности, как правило, с использование внешних знаний и данных.
- **Атаки идентификации** – вид атак логического вывода, которые позволяют в наборе данных (в том числе, обезличенном, из которого удалена персональная информация) установить кортежи, или сведения, принадлежащие конкретному субъекту.
- **Обезличивание (персональных) данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- **Обратная идентификация** - установление по защищенным данным сведений, относящихся к конкретному лицу (объекту) путем восстановления исходных данных на основе только обезличенного набора.
- **Повторная идентификация** - установление по защищенным (обезличенным или анонимизированным) данным сведений, относящихся к конкретному лицу (объекту).
- **Повторная идентификация с использованием фоновых знаний** - установление по защищенным данным сведений, относящихся к конкретному лицу (объекту) путем восстановления исходных данных с использованием внешних знаний и/или данных.

3.2 Атаки идентификации и анонимизация данных

Логический вывод и атаки идентификации. Атаки логического вывода (inference attacks) не нарушают политику доступа, но с помощью доступных агрегированных данных и фоновых знаний позволяют вывести конфиденциальную информацию о конкретном субъекте.

Повторная идентификация.

- Обратная идентификация: восстановление исходных данных X по обезличенному X' и знанию алгоритма f, $X = f^{-1}(X')$.
- С фоновыми знаниями: объединение обезличенных данных X' с внешними источниками B для установления соответствия.

Законодательные требования. Федеральный закон 152-ФЗ:

$$\text{обезличивание } X: \quad \nexists \text{ доп. инфо. } \Rightarrow \neg\big(\text{определить субъекта по } X\big).$$

Приказ РКН №996 выделяет четыре подхода к обезличиванию:

1. введение идентификаторов;
2. изменение состава и семантики данных;
3. декомпозиция;
4. перемешивание.

3.3 Методы обезличивания данных

Требования к методам. Методы должны обеспечивать:

1. Невозможность восстановления исходных X из X': $\nexists\, f^{-1}$;
2. Сохранение домена и формата: $X'_i \in \mathrm{Dom}(X_i)$;
3. Уникальность: если $X_i \neq X_j$, то $X'_i \neq X'_j$;
4. Ссылочная целостность при нескольких таблицах;
5. Применимость ко всем значениям домена;
6. Сохранение статистик: оценки по агрегатам должны быть близки.

Обратимые методы.

- **Декомпозиция**: разделение на таблицы $T_1(ID, \dots), T_2(ID, \dots)$ по суррогатному ключу ID.
- **Подстановка**: $x_i \mapsto t(x_i)$, где t задано таблицей соответствий.
- **Преобразование**:
$$V_d = F(V_u, V_r), \quad V_u = F^{-1}(V_d, V_r).$$
- **Перестановка**: обмен полями между записями; если алгоритм детерминирован, — обратимо.

Необратимые методы.

- **Замена на константу:** $x_i \to *$.
- **Округление:** $x_i \to b\,\lfloor x_i/b \rceil$, риск раскрытия $DR(X[i]) = \dfrac{1}{\log_2 m(I[i])}$.
- **Микроагрегация:** группы размера $\geq k$, замена на среднее. Риск $DR_w = \dfrac{1}{n}\sum_{k,j} w_{kj} c_{kj}$.
- **Обобщение:** замена конкретных значений на более общие (даты $\to$ месяцы).
- **Размытие (blurring):** $x_i \to x_i + \eta$, η случайно в малом диапазоне.

3.4 Концепция предположительной анонимности

Модель угадывания. Пусть $I \in \{1, \dots, M\}$ — индекс записи с псевдоидентификатором r_i, а S — наблюдаемый шумом выход. Число догадок $G(I|s)$ оптимальной стратегии минимизирует $\mathrm{E}[G(I|S)]$.

Границы по энтропии Реньи.

$$\mathrm{E}\big[G(I|S)\big]^{\rho} \;\leq\; H_\alpha(I|S),$$

где $H_\alpha(I|S) = \frac{1}{1-\alpha} \ln \sum_s \sum_i P(i,s)^\alpha$.

Gaussian-модель. При $S \mid I = i \sim \mathcal{N}(r_i, \sigma^2)$ нижняя граница

$$\mathrm{E}[G(I|S)] \;\geq\; c \sum_{i=1}^{M} \sum_{j=1}^{M} \exp\!\Big(-\tfrac{(r_i - r_j)^2}{2\sigma^2}\Big).$$

3.5 K-анонимность

Определение. Таблица T является k-анонимной, если каждая комбинация значений квазиидентификаторов Q встречается $\geq k$ раз.

Обобщение и подавление.

- Обобщение: по иерархиям VGH/DGH заменяем домен $\mathrm{Dom}(A) \mapsto$ более общий.
- Подавление: удаление отдельных кортежей, если иначе k-анонимность невозможна без сильного обобщения.

Минимальное обобщение. T_j—k-минимальное обобщение T_i, если $T_i \leq T_j$, T_j удовлетворяет k-анонимности, и нет T_z с $T_i \leq T_z < T_j$ также k-анонимного. Расстояние обобщения:

$$DV_{i,j} = [d_1, \ldots, d_n],$$

где d_ℓ — число шагов в DGH по атрибуту A_ℓ.

3.6 Дифференциальная конфиденциальность

Определение. Алгоритм A обеспечивает (ε, δ)-DP, если для любых соседних БД D_1, D_2 и всех S:

$$P[A(D_1) \in S] \;\leq\; e^{\varepsilon}\, P[A(D_2) \in S] + \delta.$$

При $\delta = 0$—ε-DP.

Механизмы.

- **Лапласовский:** добавляет шум $\mathrm{Lap}(\Delta_1/\varepsilon)$, где $\Delta_1 = \max_{D_1, D_2} |q(D_1) - q(D_2)|$.
- **Гауссовский:** добавляет шум $\mathcal{N}(0, \sigma^2)$ с $\sigma \geq \Delta_2 \sqrt{2\ln(1.25/\delta)}/\varepsilon$.
- **Экспоненциальный:** для нечисловых задач, выбор по весам $\exp(\frac{\varepsilon u(D,r)}{2\Delta u})$.

Свойства композиции.

1. Последовательная: $(\varepsilon_1, \delta_1)$ и $(\varepsilon_2, \delta_2)$ дают $(\varepsilon_1 + \varepsilon_2,\ \delta_1 + \delta_2)$.
2. Параллельная: на непересекающихся фрагментах бюджета не суммируются.
3. Расширенная: для k последовательных ε-механизмов общий бюджет $\varepsilon_{\mathrm{tot}} = O\big(\varepsilon\sqrt{k\ln(1/\delta)}\big)$.
4. Постобработка: любые $g(A(D))$ сохраняют тот же (ε, δ).

3.7 Оценка полезности и совместное применение

Метрики для специфических методов.

- **Округление:**

$$DR_i = \frac{1}{\log_2 m(I[i])}, \quad IL_i = X_i' - X_i.$$

- **Микроагрегация:** $DR_w = \dfrac{1}{n}\displaystyle\sum_{k,j} w_{kj} c_{kj}$.

- **Перестановка:**

$$DU = \frac{1}{n_T}\sum_c \big|T_p(c) - T_0(c)\big|, \quad DR = \frac{\sum I(T_0(c)=1, T_p(c)=1)}{\sum I(T_0(c)=1)}.$$

Метрики для k-анонимности.

- **Generalized IL:** $GenILoss = \dfrac{1}{n|T|}\displaystyle\sum_{i,j}\frac{U_{ij}-L_{ij}}{U_i - L_i}$.
- **Discernibility Metric:** $DM = \displaystyle\sum_{|EQ|\geq k}|EQ|^2 + \sum_{|EQ|<k}|T|\cdot|EQ|$.
- **Average EQ Size:** $C_{\text{avg}} = \dfrac{|T|}{|EQ_s|\ k}$.

Совместное применение. Сначала применяют k-анонимизацию (обобщение), затем дифференциальную приватность (малый ε) для дополнительной защиты при минимальном искажении.

4 Результаты аттестации по модулям

Прогресс учитан без финального теста, так как для него требуется платная подписка!
Результаты прохождения аттестации по темам 1-6 и общий прогресс представлены на рисунках 1 - 7

Прогресс

salimliam salimli.am@edu.spbstu.ru

Оценки

Ваша оценка по сравнению с оценкой, необходимой для прохождения этого курса.

Ваши баллы 51%

Проходной балл

Сводка по оценкам

Тип задания	Вес	Оценка	Проходной балл	Состояние
Аттестация по теме 1 [1]	10%	70.00%	70.00%	Зачтено
Аттестация по теме 2 [2]	10%	80.00%	70.00%	Зачтено
Аттестация по теме 3 [3]	10%	100.00%	70.00%	Зачтено
Аттестация по теме 4 [4]	10%	83.33%	70.00%	Зачтено
Аттестация по теме 5 [5]	10%	72.00%	70.00%	Зачтено
Аттестация по теме 6 [6]	10%	100.00%	70.00%	Зачтено

Рис. 1: Прогресс

Тема 1. Введение в курс. Задача анонимизации данных	Статус прокторинга	Оценка
▾ Аттестация по теме 1. Попытка 1	Без прокторинга	8/20
▾ Аттестация по теме 1. Попытка 2	Без прокторинга	11/20
▴ Аттестация по теме 1. Попытка 3	Без прокторинга	14/20
Оценки по заданиям: 1/1 1/1 1/1 1/1 0/1 1/1 0/1 1/1 1/1 1/1 0/1 1/1 0/1 1/1 1/1 1/1 1/1 1/1 0/1 0/1		

Рис. 2: Результаты прохождения аттестации по теме 1

Тема 2. Обезличивание данных	Статус прокторинга	Оценка
▲ Аттестация по теме 2. Попытка 1	Без прокторинга	16/20
Оценки по заданиям: 1/1 1/1 1/1 1/1 0/1 1/1 1/1 1/1 0/1 0/1 1/1 1/1 0/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1		

Рис. 3: Результаты прохождения аттестации по теме 2

Тема 3. Предположительная анонимность	Статус прокторинга	Оценка
▼ Аттестация по теме 3. Попытка 1	Без прокторинга	5/10
▲ Аттестация по теме 3. Попытка 2	Без прокторинга	10/10
Оценки по заданиям: 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1		
▼ Аттестация по теме 3. Попытка 3	Без прокторинга	0/10

Рис. 4: Результаты прохождения аттестации по теме 3

Тема 4. k-анонимность	Статус прокторинга	Оценка
▲ Аттестация по теме 4. Попытка 1	Без прокторинга	25/30
Оценки по заданиям: 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 0/1 1/1 1/1 1/1 0/1 1/1 1/1 0/1 1/1 1/1 1/1 1/1 0/1 0/1 1/1 1/1 1/1		

Рис. 5: Результаты прохождения аттестации по теме 4

Тема 5. Дифференциальная конфиденциальность	Статус прокторинга	Оценка
▲ Аттестация по теме 5. Попытка 1	Без прокторинга	18/25
Оценки по заданиям: 0/1 0/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 0/1 1/1 1/1 1/1 0/1 1/1 1/1 1/1 1/1 1/1 0/1 0/1 1/1 0/1 1/1		

Рис. 6: Результаты прохождения аттестации по теме 5

Тема 6. Оценка полезности и совместное применение методов анонимизации	Статус прокторинга	Оценка
▲ Аттестация по теме 6. Попытка 1	Без прокторинга	20/20
Оценки по заданиям: 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1		

Рис. 7: Результаты прохождения аттестации по теме 6

5 Заключение

Прохождение онлайн-курса «Анонимизация данных», автором которого является Полтавцева Мария Анатольевна, позволило ознакомиться с фундаментальными концепциями и принципами современных методов защиты персональных данных. Курс охватывал широкий спектр тем, включая основы анонимизации и обезличивания данных, методы защиты от атак идентификации, а также практические аспекты реализации механизмов конфиденциальности в информационных системах. Одной из ключевых особенностей курса стала связь изучаемых технологий с актуальными требованиями законодательства в области защиты персональных данных. Курс предоставил глубокое понимание роли современных методов анонимизации в обеспечении баланса между доступностью данных для анализа и сохранением конфиденциальности персональной информации. Особенно ценным оказалось изучение таких концепций как k-анонимность и дифференциальная конфиденциальность, которые являются основой современных подходов к защите данных. Подводя итоги, хочется отметить, что использование дистанционных образовательных технологий, на которых базировался данный курс, представляет собой важное дополнение к традиционным методам обучения. Однако, несмотря на очевидные преимущества онлайн-обучения, такие как гибкость и доступность, личное общение с преподавателем и участие в практических занятиях остаются незаменимыми для полноценного усвоения материала, особенно в области, требующей практического применения различных методов анонимизации. Онлайн-курсы, подобные этому, играют важную роль в расширении образовательных возможностей и развитии самостоятельного обучения. Они отлично дополняют основное образование, предоставляя удобные инструменты для освоения сложных концепций и навыков, востребованных в современных системах защиты информации.

6 Список источников

1. Анонимизация данных. Открытое образование: URL: https://apps.openedu.ru/learning/course/course-v1:spbstu+DATANON+spring_2025/progress(дата обращения: 15.05.2025)