Л.А. Маховиков, А.В. Линьков

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ КОНВЕРСИИ ГОЛОСА ДЛЯ СКРЫТИЯ ПЕРСОНАЛЬНЫХ ХАРАКТЕРИСТИК РЕЧИ ГОВОРЯЩЕГО В ЦЕЛЯХ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ЕГО ЛИЧНОСТИ

(Самарский университет)

Активное развитие современного информационного общества неразрывно связано с возникновением всё новых угроз информационной безопасности. Интересы личности в информационной сфере, помимо прочего, также заключаются в защите информации, обеспечивающей личную безопасность [1], что ставит проблему информационной безопасности личности в разряд наиболее актуальных на сегодняшний день.

Одним из примеров такой персональной информации, требующей защиты, является речевая информация. По имеющемуся образцу речи потенциальный злоумышленник может не только однозначно идентифицировать личность конкретного человека, но также раскрыть и другую чувствительную информацию о нём, такую как пол, расовая или этническая принадлежность, состояние здоровья, наличие акцента, текущее эмоциональное состояние и т.д. В связи с этим часто бывает полезным или даже необходимым защитить конфиденциальность личности говорящего путём скрытия или удаления связи между идентифицирующими истинный голос характеристиками и его личностью. Такую задачу в разных источниках также часто называют терминами де-идентификация (de-identification) или анонимизация (anonymization) в зависимости от того, обратимо ли такое скрытие или нет [2].

Большинство существующих на данный момент традиционных методов защиты речевой информации, такие как скремблеры, маскираторы и шифраторы, сфокусированы на защите не столько персональных характеристик говорящего, сколько на скрытии смыслового содержания речевых сообщений, передаваемых по каналам связи [3]. Подобные методы основываются на преобразовании характеристик речевого сигнала, затрудняя его разборчивость и узнаваемость для злоумышленника, а основным показателем защищенности при этом выступает речевая разборчивость [4].

Между тем, в целом ряде задач смысловое содержание речевого сообщения необходимо оставлять неизменным. Например, часто сотрудникам правопорядка в процессе проведения расследований приходится выдавать себя за других лиц во избежание раскрытия своей личности. Здесь, помимо необходимости скрытия персональных характеристик голоса, также предъявляются жесткие требования к естественности звучания преобразованного программными или аппаратными средствами голоса, который должен быть трудно отличимым от натурального. Для решения подобных задач необходимо обратить внимание на совершенно другой класс методов защиты речевой информации, в ка-

честве одного из наиболее современных примеров которого можно привести технологию конверсии голоса.

В процессе конверсии голоса речевой сигнал, произносимый одним говорящим (исходным диктором), модифицируется таким образом, чтобы он стал звучать так, как если бы он был произнесен другим говорящим (целевым диктором). При этом происходит преобразование параметров речевого сигнала исходного диктора, таких как частота основного тона, тембр, длительность звуков и пауз и некоторых других в параметры целевого в соответствии с определенным набором правил [5].

Технология конверсии голоса даёт возможность осуществить передачу речевого сообщения без риска раскрыть личность говорящего третьим лицам, при этом сохраняя натуральность преобразованной речи. Результат эффективности применения технологии конверсии голоса для обеспечения личной безопасности может быть оценён с помощью систем распознавания личности по голосу, так как если биометрическая система способна распознать голос исходного диктора в преобразованном таким образом речевом сигнале, то можно утверждать о неудаче попытки скрытия персональных речевых характеристик [6].

Разработка систем де-идентификации речевой информации на основе трансформации голоса и подтверждение их эффективности описывается в ряде научных работ. Так, в одной из статей авторами исследуется потенциал использования различных вариантов системы голосовой конверсии для преобразования 24 мужских голосов исходных дикторов в один синтезированный голос [6]. Лучший вариант системы конверсии голоса показал эффективность де-идентификации в 87,5% и 100% на двух различных системах идентификации диктора по голосу. В работе [7] тех же авторов было увеличено число участников исследования, в котором использовались голоса 95 мужских и 102 женских дикторов, а эффективность, в зависимости от сочетания вариантов применяемых систем конверсии и идентификации по голосу, могла достигать 100%.

Между тем, потенциальный злоумышленник, пытаясь сопоставить преобразованный образец речи с конкретной личностью, может обладать некоторыми знаниями об устройстве системы конверсии, с помощью которой была произведена де-идентификация голоса. Это, в свою очередь, возможно, также может повлиять на эффективность проведения такого рода атаки.

Для проверки данной теории французскими учеными был проведен ряд экспериментов с целью выяснить, как осведомленность потенциального злоумышленника о схеме де-идентификации на основе систем конверсии голоса влияет на эффективность скрытия личности. В их работе [8] исследовались три возможных сценария осведомленности атакующего: неосведомленность о факте защиты голоса, осведомленность об использующемся алгоритме преобразования, но не о значении некоторых параметров, а также полная осведомленность об алгоритме преобразования и значении параметров. Результаты экспериментов показывают, что при полной осведомленности злоумышленника ни один из рассмотренных методов конверсии голоса не способен в полной мере

защитить от раскрытия личность говорящего. В то же время, в более вероятной на практике ситуации неосведомленного или частично осведомленного злоумышленника, вполне возможно обеспечить определенную степень защиты личности диктора.

Анализ современных информационных источников позволяет сделать вывод о том, что уже при существующем уровне развития технологии конверсии голоса можно программно воспроизводить чужой голос в весьма высоком качестве, делая его сложно отличимым от естественного человеческого [9-10]. Благодаря достигнутым успехам в данном направлении исследования речевых технологий сегодня существует возможность использования преимуществ технологии конверсии голоса в целях защиты говорящего от идентификации его личности третьими лицами в случаях, когда необходимо сохранить неизменной лингвистическую составляющую речевого сообщения. Эффективность защиты в данном случае будет во многом зависеть от осведомленности злоумышленника о технических аспектах работы использующейся системы конверсии голоса, от алгоритмов функционирования и значений ее параметров. При оценке эффективности защиты необходимо учитывать как субъективную составляющую тестов на идентификацию преобразованного голоса, так и объективную, связанную с тестированием с помощью систем идентификации личности по голосу.

Литература

1. Ерошенко А.В. Информационная безопасность личности в коммуникационном процессе / А.В. Ерошенко // Материалы четвертой международной научно-практической Интернет-конференции «Стратегические коммуникации в современном мире: от теоретических знаний к практическим навыкам» [Электронный ресурс]. – URL: https://www.sgu.ru/sites/default/files/conf/files/2015/10/eroshenko_a.v._g._ryazan_informacionnaya_bezopasnost_lichnosti_v_kommunikacionnom_processe.doc (Дата обращения 14.11.2020).

2. Ribaric, S. De-identification for privacy protection in biometrics / S. Ribaric, N. Pavesic. // User-Centric Privacy and Security in Biometrics. – 2017. –P. 293-324. – DOI: 10.1049/PBSE004E.

3. Дворянкин С.В. Маскирование речевой информации: перспективные методы и средства / С.В. Дворянкин, А.А. Мишуков // "Спецтехника и связь" № 3. – 2009. – С. 46-51.

4. Устинов Р.А. Особенности современных систем защиты речевой информации / Р.А. Устинов // Безопасность информационных технологий. – 2017. – Т.24, № 4. – С. 71-79. – DOI: 10.26583/bit.2017.4.08.

5. Захарьев, В. А. Анализ подходов конверсии голоса в системах мультимедиа / В. А. Захарьев // Информационные технологии и системы 2011 (ИТС 2011) : материалы международной научной конференции, БГУИР, Минск, Беларусь, 26 октября 2011 г. / редкол.: Л. Ю. Шилин [и другие]. – Минск : БГУИР, 2011. – С. 117-118.

6. Jin, Q. Voice Converging: Speaker De-identification by Voice Transformation / Q. Jin, A.R. Toth, T. Schultz, A. W. Black // 2009 IEEE International Conference on Acoustics, Speech and Signal Processing. – 2009. – P.3909-3912. – DOI: 10.1109/icassp.2009.4960482.

7. Jin, Q. Speaker De-identification via Voice Transformation / Q. Jin, A.R. Toth, T. Schultz, A. W. Black // Proceedings of the 2009 IEEE Workshop on Automatic Speech Recognition and Understanding, ASRU 2009. – 2009. – P. 529-533. – DOI: 10.1109/ASRU.2009.5373356.

8. Lal Srivastava, B.M. Evaluating Voice Conversion-Based Privacy Protection against Informed Attackers / B. M. Lal Srivastava, N. Vauquier, M. Sahidullah, A. Bellet, M. Tommasi, E. Vincent // 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – 2020. – P.2802-2806. – DOI: 10.1109/ICASSP40776.2020.9053868.

9. Mukhopadhyay, D. All Your Voices are Belong to Us: Stealing Voices to Fool Humans and Machines / D. Mukhopadhyay, M. Shirvanian, N. Saxena // Lecture Notes in Computer Science – 2015. – Vol. 9327. – P. 599-621. – DOI: 10.1007/978-3-319-24177-7_30.

10. Neupane, A. The Crux of Voice (In)Security: A Brain Study of Speaker Legitimacy Detection / A. Neupane, N. Saxena, L. Hirshfield, S. Bratt // Network and Distributed Systems Security Symposium (NDSS 2019). – 2019. – DOI: 10.14722/ndss.2019.23206.

Р.Ш. Шарипов, Л.С. Зеленко

СИСТЕМА МОНИТОРИНГА СОСТОЯНИЙ ОТКАЗОУСТОЙЧИВОЙ РАСПРЕДЕЛЕННОЙ АРХИТЕКТУРЫ ПРОГРАММНОГО КОМПЛЕКСА «КОНТРОЛЬ ОХРАНЫ ТРУДА»

(Самарский университет)

В настоящее время многие большие программные системы являются распределенными, они состоят из нескольких автономных компьютеров, но при этом обработка информации сосредоточена не на одной вычислительной машине, а распределена между несколькими. Важным преимуществом таких систем является то, что они упрощают интеграцию различных приложений, работающих на разных компьютерах, в единую систему и хорошо масштабируются. Их размер ограничивается только размером базовой сети. Платой за эти преимущества часто является очень сложное программное обеспечение, падение производительности и особенно проблемы с безопасностью. Тем не менее, заинтересованность в построении и внедрении распределенных систем наблюдается повсеместно [1].

К числу распределенных систем относится программный комплекс (ПК) «Контроль охраны труда (КОТ)», разработанный ООО «СМС-Информационные технологии». Для того чтобы поддерживать работу такой