**УДК 004.056**

# КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ БИОМЕТРИЧЕСКОГО ГОЛОСОВОГО ОТПЕЧАТКА ОТ ВОЗДЕЙСТВИЯ КИБЕРМОШЕННИКОВ

**Герасимов В.М.** (Севастопольский государственный университет)
**Научный руководитель – Маслова М.А.**
(Севастопольский государственный университет)

**Аннотация.** Актуальность проблемы защиты данных, которые содержат в себе биометрические сведения, с каждым днём всё растёт. Использование комплексной системы защиты голосовых отпечатков поможет защитить граждан и продвинутых интернет-пользователей от воздействия кибермошенников.

**Введение.** Не для кого не секрет, что с каждым годом увеличивается количество интернет-пользователей. Так, например, в сравнении с 2020 – 2021 годом, количество интернет-пользователей по всему миру выросло на 7.62%. Не трудно предположить, что данный процесс может вызывать «обострение» в области интернет-мошенничества (чем больше пользователей в сети, тем больше мошенников воспользуются этим). Соответственно, необходимо решать один из главных вопросов – информационной безопасности пользователей в сети интернет.

Как показывает практика, наиболее возможная реализация атаки – социальная инженерия. Данным методом пользуются практически все мошенники, которые играют на эмоциях и психологии людей, тем самым получая с них прибыль. Так, например, в 2020 году на территории РФ около 62% всех мошеннических атак приходились на социальную инженерию. Тяжело представить, что произойдёт, если мошенники смогут имитировать голос жертвы, получив доступ к биометрическим данным, в частности – к голосовым данным пользователей.

**Основная часть.** При использовании кибермошенниками голосовых отпечатков, для реализации атаки методом социальной инженерии на жертву – число случаев мошенничества в сети интернет возрастёт в экспоненциальной зависимости. Естественно, в данном случае мошенниками будут использоваться всевозможные социальные сети, которые, при помощи синтезирования речи, помогут злоумышленникам получить прибыль.

Один из возможных сценариев на сегодняшний день – это взлом социальных сетей (аккаунтов), после чего анализируется страница и жизнь потенциальной жертвы (круг общения, анализ речи), синтезируется речь (по найденному образцу в аккаунте). После данных действий отправляется голосовое сообщение всем друзьям (родным и близким), с голосовыми признаками и просьбой о помощи потенциальной жертвы. Естественно, если бы вам отправили голосовое сообщение с просьбой о помощи вашего близкого человека – вы бы сразу среагировали на него, пытаясь помочь. Данная атака будет актуальна, особенно учитывая тот факт, что количество интернет-пользователей с каждым годом всё больше.

Какие социальные сети будут особенно «любимыми» для воздействия на жертв? Если обратиться к статистике, так самые популярные социальные сети на сегодняшний день, пользователями которых являются жители всего мира – WhatsApp (24%), Facebook (22%), Instagram (18.4%) и Twitter (4.8%). Данными соц. сетями пользуются для отправки как обычных сообщений, так и голосовых. Можно уже считать, какое количество пользователей могут пострадать в результате данных атак. Поэтому необходимо использовать технологии, обеспечивающие безопасность голосовых отпечатков пользователей.

Банальным, но действенным способом защиты голосовых данных является комплекс мероприятий, позволяющий создать эшелон защиты, вокруг голосовых отпечатков (аудиозаписей голосов) пользователей.

Первым самым простым, но в то же время эффективным способом сохранности голосовых данных в социальных сетях – дополнительный пароль (PIN-код) для каждого из

чатов (или особо важных диалогов, например, с родителями и близкими родственниками). При использовании данного способа, у мошенников возникнут технологические проблемы в виде подбора пароля каждого отдельного чата. Соответственно, защита предполагает сразу нескольких типов данных – голосового отпечатка, поведение потенциальных жертв и сведения об их близких.

Вторым достаточно эффективным и интересным способом является шифрование с помощью уникального ключа пользователя, который позволит зашифровать голосовое сообщение, в зависимости от чата – общий ключ шифрования данных будет различен для каждого диалога. Суть заключается в следующем, по умолчанию у каждого пользователя создаётся свой ключ (закрытый и открытый), для каждого пользователя голосовое сообщение шифруется открытым ключом пользователя, которому отправляется данной сообщение. При применении данного подхода, при несоответствии ключа – будет получен зашифрованный голосовой отпечаток, который позволяет обезопасить биометрические данные (злоумышленник получит белый шум, вместо нормальной голосовой дорожки). Данное решение позволяет защитить следующие данные – голосовой отпечаток (потенциальной жертвы, а также пользователя – с кем велась переписка). В данном способе доминирует безопасность самих голосовых отпечатков всех пользователей, пользующихся данной технологией.

Третьим способом возможного предотвращения атак является временное сохранение голосовых сообщений. Например, при отправке голосового сообщения другому пользователю можно задать временные рамки для самоуничтожения файлов. Можно будет выставить 5 минут (1 день, сутки и т. д.), после чего файл удалится, либо ограничен по количеству прослушиваний, после чего данный файл удаляется. Данный способ – как один из возможных барьеров защиты от мошенников.

Поэтому безопасность голосовых отпечатков – является перспективной технологией безопасности личности (данных) в интернете.

**Выводы.** Таким образом, данные способы комплексной системы защиты голосовых данных позволят предотвратить существенный процент кибератак, что позволит обычным интернет-пользователям так, как и раньше, без опасности для своих данных, пользоваться голосовыми технологиями, общаться и доводить информацию с помощью речи.

Внедрение данного комплекса мероприятий всех трех способов защиты, позволит улучшить позиции существующих социальных сетей, а также позволит обеспечить приложения дополнительной степенью защиты от одних из самых опасных атак в социальной инженерии. При принятии данных мер в политику безопасности – компании смогут гарантировать безопасность своих приложений от атак, чем смогут повысить рейтинг и завоевать уважение обычных пользователей, активно использующих свою речь в чате с собеседниками.

Герасимов В.М. (автор) Подпись

Маслова М.А. (научный руководитель) Подпись