АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.056.5 **DOI: 10.18413/2518-1092-2022-7-1-0-4**

Герасимов В.М.
Маслова М.А.

ВОЗМОЖНЫЕ УГРОЗЫ И АТАКИ НА СИСТЕМУ ГОЛОСОВОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: my.virus.kaspersky@gmail.com, mashechka-81@mail.ru

Аннотация
Времена меняются. Используются технологии, которые не только упрощают нам жизнь, но и помогают эффективно пользоваться всеми благами, а также достижениями человечества. Речь идёт о технологии речевого идентификации и использования голосового отпечатка, в качестве защиты пользователя. Данная технология интересна тем, что из-за распространения мобильных устройств, с применением речевых технологий, она стала доступна каждому. Многие из нас уже не могут представить жизнь без устройств, которые позволяют передавать устную (голосовую) информацию другим пользователям. Каждая новая технология несёт в себе не только положительные, но и отрицательные стороны использования средств защиты от злоумышленника. Именно поэтому необходимо учитывать все факторы той или иной технологии. В данной статье рассматривается возможные угрозы, методы воздействия на пользователя, а также анализ возможных мер для предотвращения возможных атак с использование голосового отпечатка пользователя.
Ключевые слова: угрозы голосовой идентификации; угрозы использования речевых технологий; информационная безопасность голосовых отпечатков; способы и методы защиты голосовой системы
Для цитирования: Герасимов В.М., Маслова М.А. Возможные угрозы и атаки на систему голосовой идентификации пользователя // Научный результат. Информационные технологии. – Т.7, №1, 2022. – С. 32-37. DOI: 10.18413/2518-1092-2022-7-1-0-4

Gerasimov V.M.
Maslova M.A.

POSSIBLE THREATS AND ATTACKS ON THE USER VOICE IDENTIFICATION SYSTEM

Sevastopol State University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: my.virus.kaspersky@gmail.com, mashechka-81@mail.ru

Abstract
Times change. Technologies are used that not only simplify our lives, but also help us to effectively use all the benefits, as well as the achievements of mankind. We are talking about the technology of speech identification and the use of a voice print as a user protection. This technology is interesting because due to the spread of mobile devices, using speech technologies, it has become available to everyone. Many of us can no longer imagine life without devices that allow us to transmit verbal (voice) information to other users. Each new technology carries not only positive, but also negative aspects of using means of protection against an intruder. That is why it is necessary to take into account all the factors of a particular technology. This article discusses possible threats, methods of influencing the user, as well as an analysis of possible measures to prevent possible attacks using the user's voice print.
Key words: threats to voice identification; threats to the use of speech technology; information security of voice prints; methods and techniques to protect the voice system
For citation: Gerasimov V.M., Maslova M.A. Possible threats and attacks on the user voice identification system. – T.7, №1, 2022. – P. 32-37. DOI: 10.18413/2518-1092-2022-7-1-0-4

ВВЕДЕНИЕ

С новыми возможностями – появляются новые требования. В век цифровых технологий, когда люди всё больше пользуются мобильным телефоном, всё большую популярность набирает речевые технологии (используют голос для упрощённого пользования функционалом) одним из самых перспективных технологий является использование голосовых интерфейсов [1]. Всё больше людей переходят на использование голосовых технологий, отказываясь от стандартных – текстовых.

ОСНОВНАЯ ЧАСТЬ

Согласно глобальной статистике интернета на 2021 год – около 45.3% всего населения используют голосовой поиск, а также голосовые команды [1]. Данный факт говорит о том, что всё больше людей переходят на голосовые технологии, потому что это просто, быстро, а главное – удобно.

Например, в области бизнеса для его продвижения и расширение возможностей уже мало применение рекламы, поиска новых партнеров и клиентов обычными способами, все больше внедряются современные методы, которые дают быстрый результат. По данным компании kea для удобств генеральный директор и основатель ее, расширяет свои возможности сети ресторанов, с помощью технологии голосового заказа AI (Искусственного Интеллекта) с помощью человека (см. рис. 1) [2]. Опрос Fast Casual [3] показал, что:

– 80% респондентов сообщили о голосовых устройствах для поиска ресторана;

– 61% проявили интерес к использованию голосового поиска для получения указаний в ресторан;

– 1 из 4, кто получит результат ресторана с помощью голосового поиска, посетит ресторан.

Рис. 1. Статистика эффективности голосового поиска в коммерческих целях в 2021 году, %
Fig. 1. Statistics on the effectiveness of voice search for commercial purposes in 2021, %

Данная тенденция роста голосовых технологий показывает, насколько речевые технологии – уже являются частью нашей жизни. По статистике 2021 года, использование населением устройств, которые поддерживают голосовую связь, постоянно растет (см. рис. 2) [4, 9]. Можно считать, что произошла «голосовая революция».

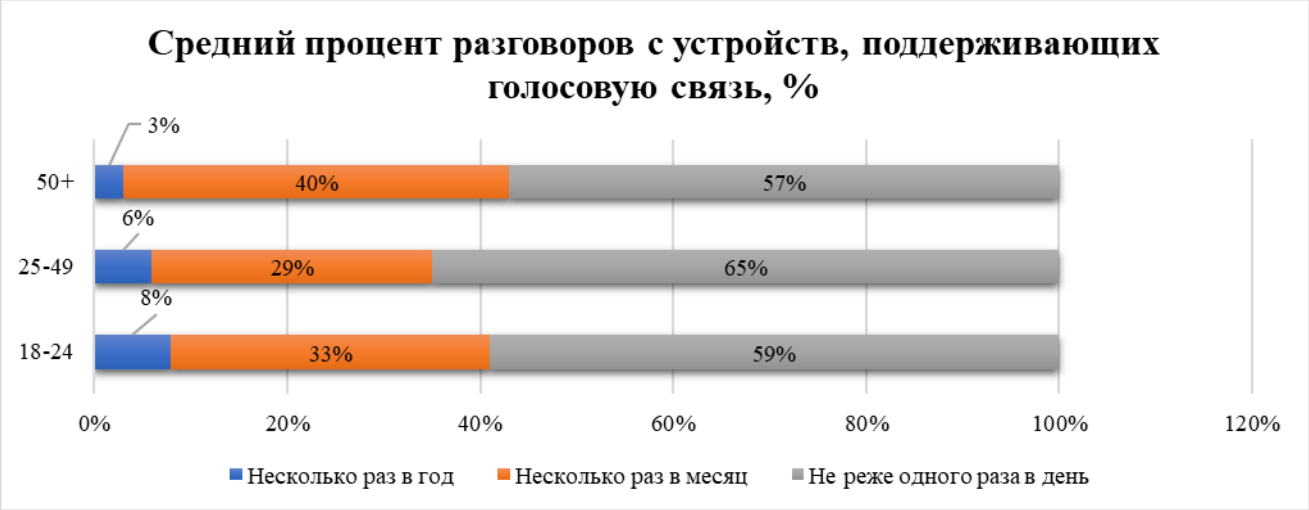

Рис. 2. Средний процент разговоров населения с устройств, поддерживающих голосовую связь, %
Fig. 2. The average percentage of conversations of the population from devices that support voice communication, %

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

С развитием данной тенденции всё больше актуальными становятся голосовая идентификация по голосу. Но какие угрозы таит в себе данная технология, если считать, что наши голоса никак не защищены. Рассмотрим возможные варианты и перспективы развития речевых технологий.

Одна из самых возможных угроз – это использование идентификации пользователя по голосу в качестве пароля, без второстепенных средств (методов защиты). Данная угроза несёт в себе следующую опасность:

1) Схожесть голосов («голосовые близнецы») – не исключены возможные совпадения голосовых признаков, с другими пользователями, соответственно, увеличивается шанс взлома, с помощью голосового отпечатка;

2) Качественная запись голоса – не исключен вариант взлома, при помощи записи голосовых характеристик пользователя. Использование записи в своих целях;

3) Пародисты, имитаторы – злоумышленники, которые обладают природной особенностью пародировать голоса, имитировать чужой тембр и тональность. При использовании своих возможностей в преступных целях, также существует возможность взлома пользователя;

4) Голосовой синтез речи – данный параметр является самым опасным из всех, т.к. сгенерирован на основании голосовых данных, соответственно, подобрать похожий голос не составит каких-либо трудностей;

Таким образом, одним из самых лучших, повышающих надёжность и безопасность входа при помощи голоса методов – это использование речевых технологий в качестве дополнительной защиты пользователя [5, 8]. Даже при использовании всех перечисленных выше угроз, придётся узнать следующие параметры – логин, пароль и сам голосовой отпечаток. Рассмотрим более подробно.

Угроза **схожести голосов** - данная угроза является максимально безобидной, в сравнении с остальными возможными угрозами. Все зависит от «случайности», получится ли зайти у одного и того же человека под одним профилем, со схожестью голоса или нет. При использовании дополнительной защиты (логин и пароль) данная угроза практически сводится к нулю, соответственно, необходимость в устранении данной угрозы является решённым.

Запись голосового отпечатка. В данном случае вероятность угрозы составляет около 30–40% (относительно всех прочих угроз). Можно считать, что данная угроза имеет смысл тогда, когда злоумышленник целенаправленно «следит» за своей целью. Локализация местности –

локальная, что означает необходимость в близком расположении к объекту, и целенаправленность на объект.

При использовании систем без текстонезависимого голосового распознавания речи, существует вероятность использования угрозы, с помощью записи голосового отпечатка. Главное решение проблемы – код-фраза (текстозваисимой системы). В данных условиях, у злоумышленника будет минимальный шанс взлома пользователя, без синтезирования речи в реальном времени (голосового синтеза речи) [6].

Пародисты (имитаторы). Данная угроза представляет собой личность, которая может сымитировать узкий круг людей, но, все же, является опасной угрозой. Метод очень похож, как при записи голосового отпечатка, но, к использованию тестозависимой системы, он равнодушен, хоть и возможность реализации его очень мала, все же риск при этом существует и составляет около 40–65% (относительно всех возможных угроз).

Для устранения возможной угрозы необходима дополнительная защита – использование логина, пароля и текстозависимой системы. Считается, что при использовании эффективного пароля, злоумышленник не сможет использовать уязвимость системы речевого распознавания пользователя. Также при рассмотрении данной угрозы, имеет место быть – использование системы с подозрительным входом, которые при входе с нового устройства или переборе пароля, попросит пользователя поменять пароль и изменить голосовой отпечаток.

Голосовой синтез речи. На сегодняшний день – эта технология, которая сразу, при условии всех остальных параметров имеет вероятность угрозы 65–100%, данный параметр зависит от злоумышленника и его уровня подготовки:

– во-первых, если злоумышленник использует такие средства, как: слежка, утечка данных и производительная вычислительная мощность, то при правильном использовании шансы очень велики.

– во-вторых, параметры анализа возможных угроз зависят от пользователя и системы предварительной проверки регистрации – система, которая проверяет пароль на стойкость от взлома (см. рис. 3) [7].

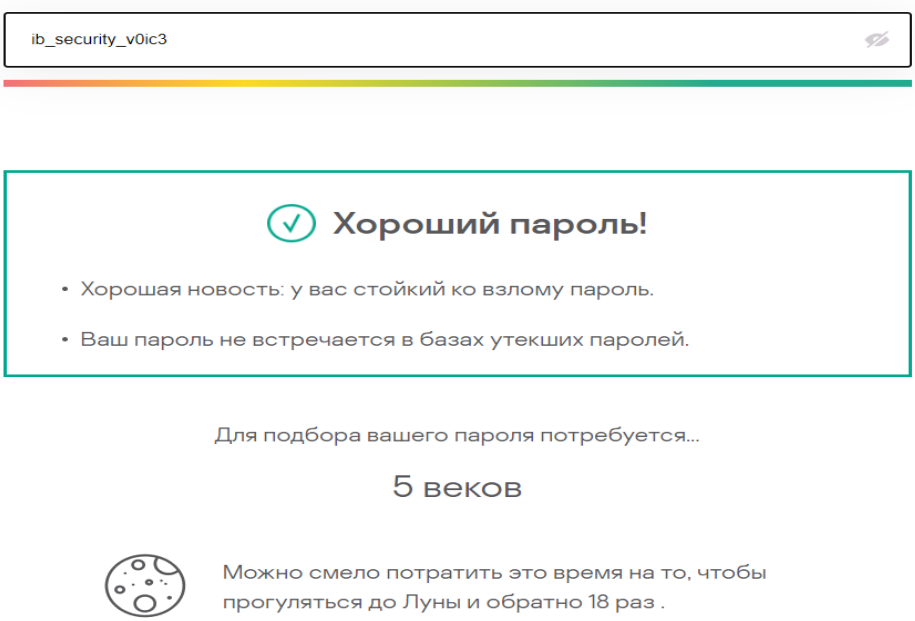

Рис. 3. Пример проверки хорошего пароля
Fig. 3. Example of checking a good password

Таким образом, данную угрозу можно устранить при условии текстозависимой системы и устойчивого пароля пользователя, тогда данные угрозы не имеют места быть и вероятность их реализации будет стремиться к нулю [10].

ЗАКЛЮЧЕНИЕ

Технологии развития голосовой идентификации не гарантируют 100% от взломов пользователей в сети, но именно данная технология направлена на то, чтобы уменьшить вероятность взломов обычных пользователей в сети. С данной технологией, в качестве дополнительной защиты, уменьшится количество взломов аккаунтов.

Преимущества данной технологии заключается в простоте использования и повышения надёжности защиты от «обычных угроз». Даже пользователи с простым паролем, имеющие голосовую идентификацию, могут повысить свою безопасность в 1,5 раза. Ведь при данном условии злоумышленникам становится все труднее получить доступ к данным пользователям, т.к. уже необходимо подобрать не только пароль, но и голосовой отпечаток, и, следовательно, шанс ошибки взлома кардинально увеличивается.

Таким образом, можно сделать вывод, что угрозы голосовой идентификации все же существуют, но все-таки их тоже можно защитить, но при этом данная технология приносит в современный мир значительную пользу в повышении защиты от взломов пользователей, т.к. все больше и больше возрастает спрос на использование речевых технологии в повседневной деятельности.

Список литературы

1. Digital 2021: последние новости о «состоянии цифровых технологий» - We Are Social UK (https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital/);
2. https://www.forbes.com/sites/forbestechcouncil/2021/05/07/how-voice-ai-is-changing-the-way-people-order-food/?sh=52b2c6af7709
3. https://www.fastcasual.com/news/study-1-in-4-consumers-who-get-a-restaurant-result-in-voice-search-visit-that-restaurant/;
4. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/voice-assistants.html;
5. Костиков В.А., Маслова М.А. Использование системы голосовой идентификации в качестве дополнительной защиты пользователя // 17-я Международная молодёжная научно-техническая конференция «Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2021», 11 — 15 октября 2021 г., Севастополь, Российская Федерация, с.223-224;
6. Маслова М.А. Усовершенствование системы защиты данных в информационных системах методом голосовой биометрии //Новая наука: Стратегии и векторы развития. 2016. № 2-1 (64). С. 20-22;
7. Password Check | Kaspersky (https://password.kaspersky.com/ru/).
8. Devitsyna S., Eletskaya T., Meshkov A. Developing facial recognition software to control access to campus facilities // CEUR Workshop Proceedings. 2. Сер. "InnoCSE 2019 – Proceedings of the 2nd Workshop on Innovative Approaches in Computer Science within Higher Education" 2019. С. 68-76;
9. Девицына С.Н., Каргин А.С., Балабанова Т.Н. Создание модели нейросети для аутентификации пользователя по голосу // Информационные технологии в науке, образовании и производстве (ИТНОП-2020). сборник материалов VIII Международной научно-технической конференции. Белгород, 2020. С. 38-42;
10. Девицына С.Н., Елецкая Т.А., Балабанова Т.Н., Гахова Н.Н. Разработка интеллектуальной системы биометрической идентификации пользователя // Научные ведомости Белгородского государственного университета. Серия "Экономика. Информатика". 2019. Т. 46. № 1. С. 148-160. DOI: 10.18413/2411-3808-2019-46-1-148-160.

References

1. Digital 2021: The Latest on the 'State of Digital' – We Are Social UK (https://wearesocial.com/uk/blog/2021/01/digital-2021-the-latest-insights-into-the-state -of-digital/)

2. https://www.forbes.com/sites/forbestechcouncil/2021/05/07/how-voice-ai-is-changing-the-way-people-order-food/?sh=52b2c6af7709

3. https://www.fastcasual.com/news/study-1-in-4-consumers-who-get-a-restaurant-result-in-voice-search-visit-that-restaurant/

4. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/voice-assistants.html

5. Kostikov V.A., Maslova M.A. Using the voice identification system as additional user protection // 17th International Youth Scientific and Technical Conference "Modern problems of radio electronics and telecommunications, RT-2021", October 11 - 15, 2021, Sevastopol, Russian Federation, P. 223-224

6. Maslova M.A. Improving the data protection system in information systems using voice biometrics // New Science: Strategies and vectors of development. 2016. No. 2-1 (64). pp. 20-22

7. Password Check | Kaspersky (https://password.kaspersky.com/ru/)

8. Devitsyna S., Eletskaya T., Meshkov A. Developing facial recognition software to control access to campus facilities // CEUR Workshop Proceedings. 2. Ser. "InnoCSE 2019 – Proceedings of the 2nd Workshop on Innovative Approaches in Computer Science within Higher Education" 2019. P. 68-76

9. Devitsyna S.N., Kargin A.S., Balabanova T.N. Creation of a neural network model for user authentication by voice // Information technologies in science, education and production (ITNOP-2020). collection of materials of the VIII International Scientific and Technical Conference. Belgorod, 2020. P. 38-42

10. Devitsyna S.N., Eletskaya T.A., Balabanova T.N., Gakhova N.N. The development of intelligent biometric identification system user // Belgorod State University. Scientific Bulletin. Series: Economics. Information technologies. 2019. T. 46. № 1. P. 148-160. DOI: 10.18413/2411-3808-2019-46-1-148-160

Герасимов Виктор Михайлович, студент четвертого курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Gerasimov Viktor Mikhailovich, fourth-year student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, senior lecturer of the Department Information security, Institute of Radioelectronics and Information security