УДК 004

Давлетшин Б.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

МЕТОД НУЛЕВОГО ДОВЕРИЯ (ZERO TRUST) МЕЖДУ ЛЮДЬМИ КАК ОТВЕТНАЯ МЕРА НА РАСПРОСТРАНЕНИЕ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Аннотация. В статье рассматривается применение концепции Zero Trust и перенос принципов кибербезопасности на уровень межличностного общения в контексте голосовых коммуникаций.

Ключевые слова: нулевое доверие, телефонное мошенничество, социальная инженерия, поведенческая аутентификация, цифровая безопасность.

Современные цифровые технологии, с одной стороны, упрощают повседневную коммуникацию и обеспечивают удобство взаимодействия, а с другой – создают широкие возможности для злоумышленников. В последние годы наблюдается рост количества телефонных мошенничеств, особенно с использованием подмены номеров, социальных манипуляций и технологий искусственного интеллекта (ИИ), таких как генерация голоса.

Традиционные средства защиты, основанные на доверии к идентификатору звонящего, становятся недостаточными. В этих условиях возрастает потребность в применении более строгих и универсальных моделей безопасности. Одной из таких моделей является концепция Zero Trust Security (модель нулевого доверия), которая предполагает отсутствие автоматического доверия к любому субъекту взаимодействия без предварительной проверки его подлинности [1].

Актуальность исследования обусловлена необходимостью адаптации принципов Zero Trust к голосовой коммуникации, как в личной, так и в деловой среде. В условиях постоянного роста количества и сложности мошеннических схем важно сформировать устойчивые поведенческие паттерны защиты от угроз [2].

Метод Zero Trust был изначально разработан для защиты цифровой инфраструктуры и ИТ-систем, где каждый пользователь и устройство проходят обязательную аутентификацию и проверку доступа. Однако его применение к сфере голосовых коммуникаций между людьми ранее не рассматривалось системно. Новизна заключается в переносе принципов цифровой безопасности на уровень обычной телефонной беседы.

Ключевые аспекты новизны [3]:

– формирование концепции «не доверяй – проверяй» в бытовом телефонном общении;

– внедрение поведенческой и голосовой аутентификации при голосовых вызовах;

– объединение технологических инструментов (антиспам-фильтров, распознавания речи) с социально-психологическими механизмами (обучение, кодовые слова, критическое мышление);

– учет возможности фальсификации голоса с помощью ИИ как нового фактора риска.

Данная адаптация делает подход Zero Trust универсальным инструментом противодействия мошенничеству как в цифровой, так и в человеческой плоскости коммуникаций.

Актуальные угрозы телефонных коммуникаций можно классифицировать по нескольким направлениям:

1. Подмена номера (Caller ID Spoofing): Используя технологии VoIP и специальное программное обеспечение, мошенники могут звонить с номеров, визуально совпадающих с номерами банков, госучреждений, родственников или коллег. Это создает иллюзию легитимности и повышает вероятность доверия со стороны жертвы.

2. Голосовые подделки (Deepfake Voice): Развитие ИИ позволило создавать фальсификации голосов, практически неотличимые от оригинальных. Это используется для атак в бизнес-среде (например, фальшивый звонок от «директора» с просьбой перевести деньги) или в частной жизни (имитация голоса ребенка с просьбой о помощи).

3. Социальная инженерия: Используется для создания чувства срочности, паники, доверия или страха. Примеры включают звонки от «службы безопасности банка», «следователя», «медработника» или «внука» с мольбами о срочной помощи. Часто используется сценарий, в котором жертва должна действовать немедленно, не раздумывая.

4. Фишинг по телефону (Vishing): Выманивание паролей, одноразовых кодов и других данных. Отличие от традиционного фишинга заключается в том, что атака происходит в реальном времени и часто подкреплена манипулятивной речью и подменой номера.

5. Технические уязвимости: Использование уязвимостей в системах VoIP, недостаточной защиты приложений, отсутствие защиты SIM-карт и уязвимости в прошивке телефонов также могут использоваться злоумышленниками для компрометации связи.

Для применения модели нулевого доверия в голосовых коммуникациях необходимо формировать устойчивые принципы взаимодействия, основанные на проверке, а не на доверии. Предлагаются следующие рекомендации:

1. Недоверие к внешним признакам достоверности: Не следует полагаться на номер, отображаемый на экране телефона, голос собеседника или даже содержание разговора. Всегда необходима проверка источника информации.

2. Использование вторичных каналов проверки: При сомнениях следует завершить разговор и связаться с предполагаемым собеседником через альтернативный канал связи – мессенджер, электронную почту, личную встречу.

3. Введение кодовых слов: В кругу семьи или в организации можно договориться об использовании заранее определенных кодовых фраз для верификации личности. Такие слова не должны быть очевидными и должны периодически меняться.

4. Анализ поведенческих признаков: Несвойственный стиль общения, агрессия, попытки вызвать панику, навязывание решений – все это признаки мошеннической атаки. Zero Trust требует внимательного наблюдения за такими проявлениями.

5. Отказ от передачи конфиденциальных данных: Под предлогом безопасности мошенники часто просят предоставить код из SMS, номер карты или CVV. Согласно Zero Trust, никакие данные не должны передаваться по инициативе звонящего.

6. Технологическая защита: Использование приложений для идентификации звонков (например, Truecaller), блокировка неизвестных и скрытых номеров, фильтрация звонков по ключевым признакам.

7. Обучение и профилактика: Регулярное проведение обучающих мероприятий и тренингов, создание корпоративных стандартов коммуникации, разработка внутренних инструкций по верификации личности при звонках.

Рассмотрим ряд реальных кейсов, подтверждающих необходимость внедрения Zero Trust:

– случай в Германии (2024): Мошенники, подделав голос дочери пенсионерки, сообщили о ДТП и необходимости срочного перевода крупной суммы. Женщина спаслась от потери средств только благодаря привычке перезванивать близким и задавать уточняющие вопросы;

– инцидент в Великобритании (2023): Руководитель компании получил звонок от «директора» с просьбой о переводе средств. Грамотная проверка голоса и дополнительное подтверждение по электронной почте позволили предотвратить финансовые потери;

– финансовый сектор России (2022): Один из банков внедрил голосовую биометрию при входящих звонках от клиентов. Это позволило за год сократить количество успешных мошеннических звонков на 38 %.

Модель Zero Trust, адаптированная к телефонной коммуникации, предоставляет мощный инструмент противодействия современным угрозам. Переход от доверия к проверке позволяет минимизировать влияние манипулятивных и технически сложных атак.

Комплексный подход, включающий технологические средства, поведенческие практики и образовательные меры, делает метод нулевого доверия универсальным и масштабируемым [4]. Применение этого подхода способствует формированию цифровой гигиены общения и защите интересов граждан, организаций и общества в целом.

Перспективы дальнейших исследований включают разработку автоматизированных систем голосовой аутентификации, интеграцию Zero Trust в государственные стандарты связи, а также расширение практики обучения в образовательных учреждениях и организациях.

Список использованных источников:

1. Zero Trust Maturity Model. U.S. Department of Homeland Security. // CISA. URL: https://www.cisa.gov/zero-trust-maturity-model.

2. Как избежать атаки с использованием социальной инженерии // Kaspersky Lab. URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks.

3. Нейросети: как мошенники используют ИИ для обмана // Коммерсант. URL: https://www.kommersant.ru/ /doc/6616414.

4. Многоагентные системы как технологическая база реализации концепции нулевого доверия / С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.С. Исмагилова // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2024. № 3. С. 116–123. DOI 10.18137/RNU.V9187.24.03.P.116.

Davletshin B.M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

THE ZERO TRUST METHOD BETWEEN PEOPLE AS A RESPONSE TO THE SPREAD OF ARTIFICIAL INTELLIGENCE FOR TELEPHONE FRAUD

Abstract. The article examines the application of the Zero Trust Security concept and the transfer of cybersecurity principles to the level of interpersonal communication in the context of voice communications.

Keywords: zero trust, phone fraud, social engineering, behavioral authentication, digital security.