и скорости обработки цифровой информации аудипотока, с возможностью остановки записи, проверки правильности введенной информации, корректировки данных, возобновления записи с заданного места. Также возможно добавление новых функций, таких как возможность анализа тональности речи или определение эмоционального состояния пользователя на основе аудиопотока. Важно также обеспечить безопасность и конфиденциальность данных, особенно в медицинской сфере, что может потребовать внедрения механизмов шифрования и защиты информации.

Заключение. Применение новых технологий для автоматизации рутинной работы по вводу цифровых данных, характеризующих типовые объекты, позволило создать приложение для управления данными аудиопотока, позволяющее осуществить ввод данных, обеспечить контроль за корректностью введенной информацией и оперативное управление полученными данными с целью их анализа и интерпретации.

Полученный опыт использования среды разработки PyCharm для создания, отладки и тестирования приложения для структурирования и сохранения цифровых данных аудиопотока о параметрах пациентов медицинского учреждения может быть использован при создании аналогичных программных средств для управления данными аудиопотока в других предметных областях (биологии, лесном хозяйстве, производстве и др.), позволив удовлетворить потребности современных пользователей. В этом заключается универсальность реализованного программного обеспечения.

Д. А. Шумило
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Васькевич**, ст. преподаватель

ОСНОВНЫЕ КОНЦЕПЦИИ МОДЕЛИ БЕЗОПАСНОСТИ ZERO TRUST

“Zero Trust” – набор инструкций для обеспечения безопасности, разработанный Джоном Киндервегом (бывший аналитик исследовательской компании Forrester Research и старший вице-президент ON2IT). Эта концепция приобрела особую популярность в последнее время из-за участившихся кибератак. В данной работе будет представлен анализ основных идей, принципов и преимуществ модели Zero Trust.

Как следует из названия («Нулевое доверие»), модель предполагает недоверие к любому пользователю и, следовательно, аутентификацию при каждом запросе доступа к любому ресурсу. По сути, эта концепция размывает границы понятия «периметр», так как в современном мире невозможно защитить все данные и ресурсы, расположив их в одном большом «замке со рвом». Следовательно, более простым решением может быть разбиение сети и ресурсов на отдельные узлы, каждый из которых будет иметь свои собственные политики безопасности и правила доступа.

В рамках стратегии «нулевого доверия» выделяются пять основных областей и три принципа. Основные области включают:

1. Данные: Основная цель злоумышленников – это данные, поэтому первоочередной областью внимания в концепции «нулевого доверия» является способность к анализу, защите и классификации данных (включая вычислительные ресурсы). Для обеспечения защиты доступа к данным используются политики, которые учитывают параметры идентификатора пользователя и системы, к которой необходим доступ, а также MFA (Многофакторная Аутентификация), примером которой может служить 2FA. Важным элементом являются также поведенческие метрики.

2. Сети: для успешной кражи информации преступникам необходимо перемещаться внутри сети, поэтому основной целью на втором этапе является максимальное усложнение перемещений за счет сегментации, изоляции и контроля сети с помощью межсетевых экранов.

3. Пользователи: Человеческий фактор часто является самой большой проблемой в системе безопасности. Важно контролировать и ограничивать доступ к ресурсам как внутри корпоративной сети, так и в интернете. В этом контексте динамическая аутентификация пользователей становится ключевым элементом, который следует поддерживать до момента получения доступа. Это снизит воздействие пользователей на чувствительные части сети. Так же для защиты пользователей и инфраструктуры можно применять CASB, IDS, IPS, шлюзы электронной почты с защитой по периметру и другие средства.

4. Нагрузка: под нагрузкой подразумевается полный стек программного обеспечения (включая гипервизоры и т. д.). Долгое отсутствие патчей безопасности создает идеальный вектор атаки.

5. Устройства: быстро набирающие популярность устройства «интернета вещей» также представляют собой потенциальную точку атаки.

Основные принципы включают: аутентификацию и проверку всех прав доступа к каждому ресурсу, применение модели минимальных привилегий и управление доступом, мониторинг и регистрация всех действий и элементов, находящихся за пределами защитного периметра.

Использование “zero trust” несет в себе много преимуществ. Применение принципов безопасного проектирования помогает уменьшить риски, связанные с постоянными угрозами. Технологии, включающие встроенную изоляцию пользователей и доступ с ограниченными привилегиями, помогают удовлетворять нормативные требования и политики конфиденциальности. Эффективное управление учетными записями позволяет организациям усилить контроль над доступом пользователей, что способствует снижению рисков нарушения безопасности как внутри, так и за пределами организации. Так же использование этой концепции увеличивает гибкость в управлении правами доступа (например, при изменении круга задач сотрудников).

В качестве примера использования “zero trust” можно выделить концепцию ZTNA (Zero Trust Network Access) и фреймворк SASE (Secure Access Service Edge) от компании Gartner, разработанные на основе вышеупомянутой модели. Оба решения снижают поверхность атаки, используя зашифрованные one-to-one соединения, и обеспечивают безопасность как локальных корпоративных сетей, так и облачных сервисов.