УДК 004.42

АВТОМАТИЗАЦИЯ СИСТЕМЫ МОНИТОРИНГА ПОЛЬЗОВАТЕЛЬСКИХ УСТРОЙСТВ В ЛОКАЛЬНОЙ СЕТИ

Николаева О.С. ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», **Федоров Я.Н.** ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Научный руководитель – преподаватель Кривоносова Н.В.

ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Введение. Мониторинг пользовательских устройств в локальной сети является одним из распространённых методов обеспечения информационной безопасности от внутренних угроз. Существующие на сегодняшний день решения зачастую имеют избыточный функционал, что делает данные системы не всегда доступными по стоимости для предприятий малого и среднего бизнеса. Доклад будет посвящён обзору архитектуры системы мониторинга пользовательских устройств в локальной сети, средствам и технологиям разработки. Докладчиками будет представлен минимальный демонстрационный объект системы мониторинга, разработанный на языке программирования C# и на сервере баз данных PostgreSQL.

Основная часть. Система мониторинга действий пользователя — программный комплекс, позволяющий отслеживать действия сотрудника за рабочим местом. Данная система осуществляет мониторинг рабочих операций пользователя на предмет их соответствия корпоративным политикам. Основная функция мониторинга — протоколирование всех действий пользователя. Это позволяет своевременно обнаружить утечку важной информации за пределы организации, а также при необходимости восстановить последовательность действий пользователя для более эффективного решения критических ситуация и разногласий относительно продуктивности работы сотрудника. Автоматизация систем мониторинга для современных предприятий наиболее актуальна в связи с повышением доли умышленных нарушений внутреннего характера.

Для реализации данного проекта, с возможностью дальнейшей масштабируемости решения, и выноса ресурсоемких задач на сторону сервера, оптимальным решением является четырёхкомпонентная архитектура, состоящая из:

1. Компонент-приложение на стороне агента — представляет из себя консольное приложение, работающее в скрытом от пользователя режиме, собирающее и отправляющее информацию на сервер. На этом компоненте располагаются основные вычисления, связанные со сбором данных; [1]
2. Компонент-приложение на стороне администратора — представляет из себя WPF-приложение, доступное только администратору. Управление системой производится с помощью графических элементов. На этом компоненте располагаются основные вычисления, связанные с созданием и редактированием правил мониторинга системы. [1]
3. Компонент-база данных — база данных под управлением СУБД PostgreSQL, в которой хранятся все данные, собранные на компонентах-приложениях. [2]
4. Компонент-Web API – приложение на сервере, обеспечивающее взаимодействие компонентов-приложений с компонентом-базой данных. Для создания Web API был выбран архитектура REST (Representational state transfer). Обмен данными с приложениями идет посредством JSON, а с базой данных настроено взаимодействие через SQL-запросы. [3]

Выводы. В ходе выполнения данного проекта были изучены существующие решения по автоматизации систем мониторинга пользовательских устройств в локальной сети, на основании этого был произведён анализ и разработан макет данной системы.

Список использованных источников:

1. Хорев П.Б. Объектно-ориентированное программирование с примерами на C#. Учебное пособие. - 4-е изд. - Москва: Форум, 2020. - 200 с. – С. 44 – 186.
2. Моргунов Е.П. PostgreSQL. Основы языка SQL. - Санкт-Петербург: БХВ, 2019. - 340 с. - С. 51-226; С. 293– 217
3. Умрихин Е.Д. Разработка веб-приложений с помощью ASP.Net Core MVC. - Санкт-Петербург: БХВ, 2023. - 416 с. - С. 46-68; С. 180– 208