УТВЕРЖДЕН
RU.СГПВ.508110.001-01 92 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ СБОРА И ИССЛЕДОВАНИЯ ИНФОРМАЦИИ О ВЫДАВАЕМЫХ SSL-СЕРТИФИКАТАХ В СЕТИ ИНТЕРНЕТ

IoTSensor

Описание функциональных характеристик

RU.СГПВ.508110.001-01 92 01

Листов 11

2021

Инв. № подл.	Подпись и дата	Взам. инв.№	Инв. № дубл.	Подпись и дата

АННОТАЦИЯ

Настоящий документ содержит описание программного обеспечения для сбора и исследования информации о выдаваемых SSL-сертификатах в сети Интернет (далее – ПО IoTSensor, программа) и его функциональных характеристик.

Документ состоит из трех разделов, в которых раскрываются основные вопросы применения, структуры и функционирования ПО IoTSensor. Кроме того, в документе рассматриваются технические характеристики аппаратных средств, необходимых для функционирования программы.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

В настоящем разделе приведены обозначение и наименование программы, программное обеспечение, необходимое для функционирования программы, а также языки программирования, на которых написана программа.

1.1. Обозначение и наименование программы, сведения о разработчике

Наименование и обозначение – "Программное обеспечение для сбора и исследования информации о выдаваемых SSL-сертификатах в сети Интернет" (далее – ПО IoTSensor, программа).

Разработчик программы – ФГАНУ НИИ "Спецвузавтоматика", 344003, г. Ростов-на-Дону, ул. Города Волос, д. 6.

1.2. Программное обеспечение, необходимое для функционирования программы

ПО IoTSensor функционирует под управлением операционной системы (далее – ОС) Ubuntu Server версии 18.04 и выше.

Для работы программы требуется система управления базами данных (далее – СУБД) ClickHouse версии не ниже 20.12.3.3.

СУБД ClickHouse внесена в Единый реестр российских программ для электронных вычислительных машин и баз данных, запись в реестре № 5354 от 06.05.2019.

1.3. Язык программирования, на котором написана программа

ПО IoTSensor написано на языке программирования Golang, для взаимодействия с СУБД использует разновидность языка запросов SQL, разработанного для СУБД ClickHouse.

1.4. Основные характеристики программы

ПО IoTSensor обладает следующими характеристиками:

– объем установочного пакета – 5,1 Мб;

– объем дополнительных зависимостей, разворачиваемых при установке ПО IoTSensor (СУБД ClickHouse), – 439 Мб;

– среда исполнения программы – ОС Ubuntu Server версии 18.04 и выше;

– обязательное наличие СУБД ClickHouse (устанавливается автоматически при установке программы);

– при скорости соединения с информационной сетью Интернет, равной 100 мегабит в секунду, скорость получения и обработки данных составляет порядка 100 000 сертификатов в минуту.

2. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

ПО IoTSensor представляет собой программу, функционирующую в фоновом режиме в виде сервиса системы и непрерывно собирающую данные из публично доступных реестров Certificate Transparency Logs.

2.1. Классы решаемых задач

ПО IoTSensor предназначено для решения следующих задач:

- загрузка сертификатов безопасности;
- сохранение сертификатов в базу данных;
- просмотр и поиск сертификатов в базе данных.

2.2. Функциональное назначение программы

Назначением программы является загрузка сертификатов, их обработка, создание и хранение массива данных сертификатов безопасности для последующего решения разноплановых задач, таких как поиск сертификатов, принадлежащих конкретным доменам, издателям и т. д. Сформированный массив данных можно использовать для решения статистических и аналитических задач.

2.3. Сведения о функциональных ограничениях на применение

ПО IoTSensor требует для функционирования не менее 8 гигабайт оперативной памяти и не менее 4 процессорных ядер.

При меньших объемах заявленных характеристик программа и связанные с ней программные средства могут вызывать повышенную нагрузку на вычислительные ресурсы и общее замедление всех выполняемых на вычислительном средстве задач.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

В настоящем разделе указаны алгоритм программы, используемые методы, структура программы с описанием функций составных частей и связи между ними, связи программы с другими программами.

Описание логической структуры программы выполняют с учетом текста программы на исходном языке.

3.1. Алгоритм выполнения программы

Алгоритм выполнения программы состоит из следующих этапов:

1) запуск программы;
2) подключение к базе данных;
3) чтение сертификатов;
4) сохранение сертификатов в базу данных;
5) завершение.

3.2. Используемые методы

В ПО IoTSensor используются методы взаимодействия с информационной сетью Интернет по протоколу HTTP посредством стандартных библиотек языка Golang. Методы взаимодействия с СУБД ClickHouse и web-интерфейсом также являются реализацией стандартных библиотек языка Golang для этих решений.

3.3. Структура программы с описанием функций составных частей и связи между ними

В структуру ПО IoTSensor входят СУБД ClickHouse и сервис для сбора данных о сертификатах безопасности.

Функции СУБД ClickHouse:

- хранение данных;
- сжатие данных;
- агрегация данных по ключам сортировки.

Функции сервиса для сбора данных:

– считывание логов данных;
– перевод данных в формат схемы СУБД ClickHouse;
– запись в хранилище данных СУБД ClickHouse;
– поиск данных.

Функцией логов данных является предоставление данных для последующего чтения.

3.4. Связи программы с другими программами

Типовая структурная схема связей между частями программы приведена на рисунке 1.

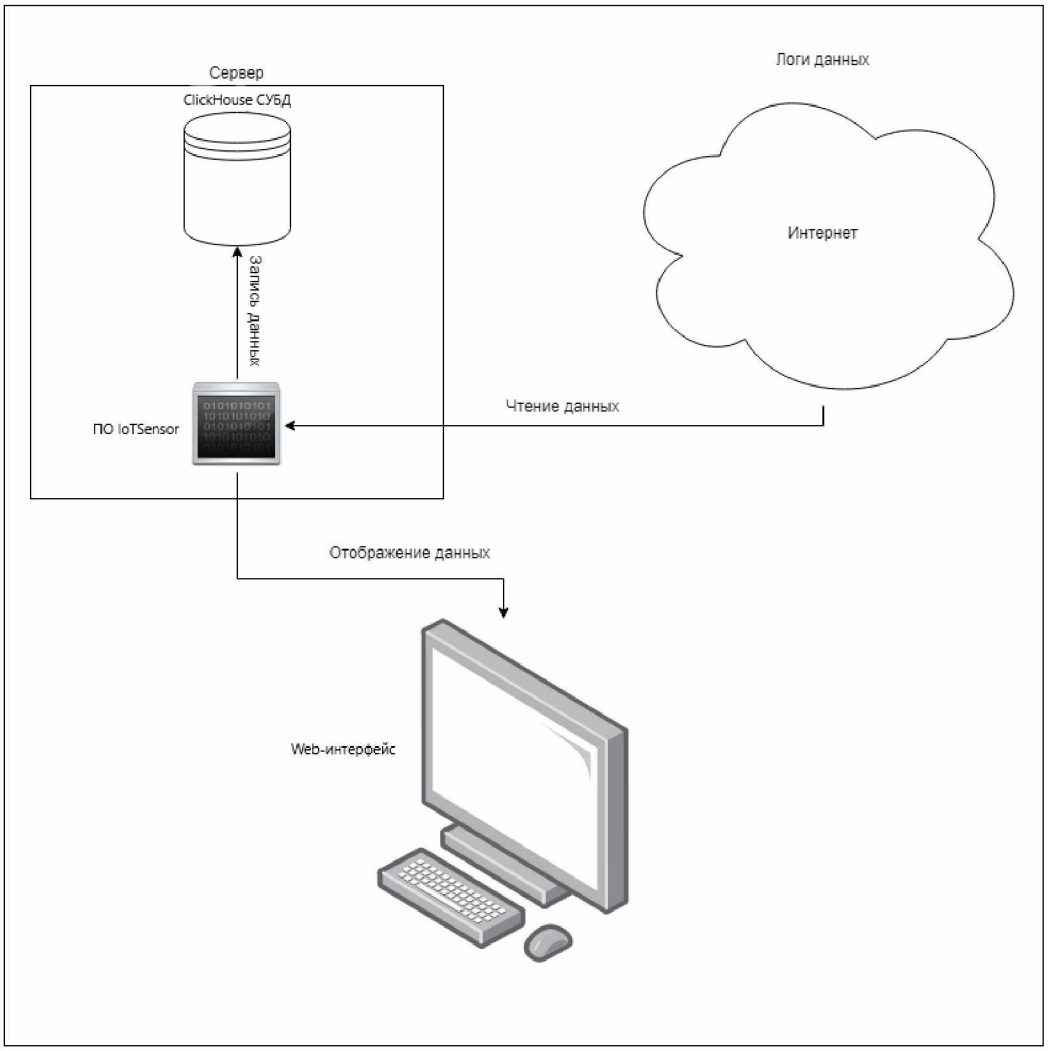

Рисунок 1 – Типовая структурная схема связей между частями программы

Связь между СУБД ClickHouse и сервисом для сбора данных осуществляется путем:

– записи данных;

– чтения данных по запросу пользователя.

Связь между логами данных и сервисом для сбора данных осуществляется путем чтения данных из реестров Certificate Transparency Logs, расположенных в информационной сети Интернет.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе приняты следующие сокращения:

HTTP	–	Hyper Text Transfer Protocol;
SQL	–	Structured Query Language;
TLS	–	Transport Layer Security;
ОС	–	операционная система;
ПО	–	программное обеспечение;
СУБД	–	система управления базами данных.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					