

Дата диод для безопасной передачи данных критической инфраструктуры

Эффективный способ безопасного экспорта данных

Zhanibek Yeskendir
AIMI Automation

О компании

AIMI Automation

www.aimi-automation.com



Молодая 100% казахстанская компания

20 реализованных проектов

Ряд зарубежных проектов, в том числе в США

Собственные разработки:
SmartDabyl, LogView,
DataDiode

Наша команда

Команда **AIMI** состоит из профессионалов. Некоторые перечислены ниже.

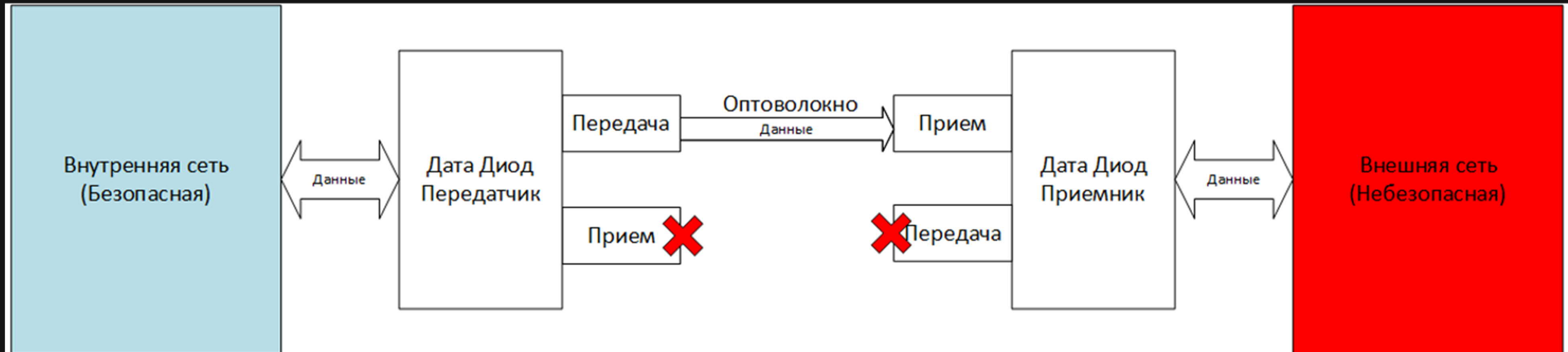
Мы верим в то, что инновационные продукты создаются профессионалами и не появляются из неоткуда

АБЗАЛ КАНАЕВ		ЖАНИБЕК ЕСКЕНДИР		ЕЙВАЗ МАММАДЛИ
Менеджер проектов. 13 лет опыта в ТШО. Награды: ТШО, Honeywell, KazEnergy Сертификаты: EPKS, SM, TPS		Развитие бизнеса. 13 лет опыта работы в отрасли. Катар, РФ, Восточная Европа, Казахстан Награды: Chevron, Honeywell, KazEnergy Сертификаты: TUV FSEng, EPKSL4		Эксперт по кибербезопасности. 18 лет опыта в отрасли. Награды: Honeywell, EY Сертификаты: MCSA, CEH, CRISC, CISM, Cisco, VMWare

Что такое дата диод?



Дата диод ограничивает сетевой трафик в одном направлении при этом гарантирует физическую невозможность передачи данных в обратном направлении.



Преимущества и актуальность ИСПОЛЬЗОВАНИЯ

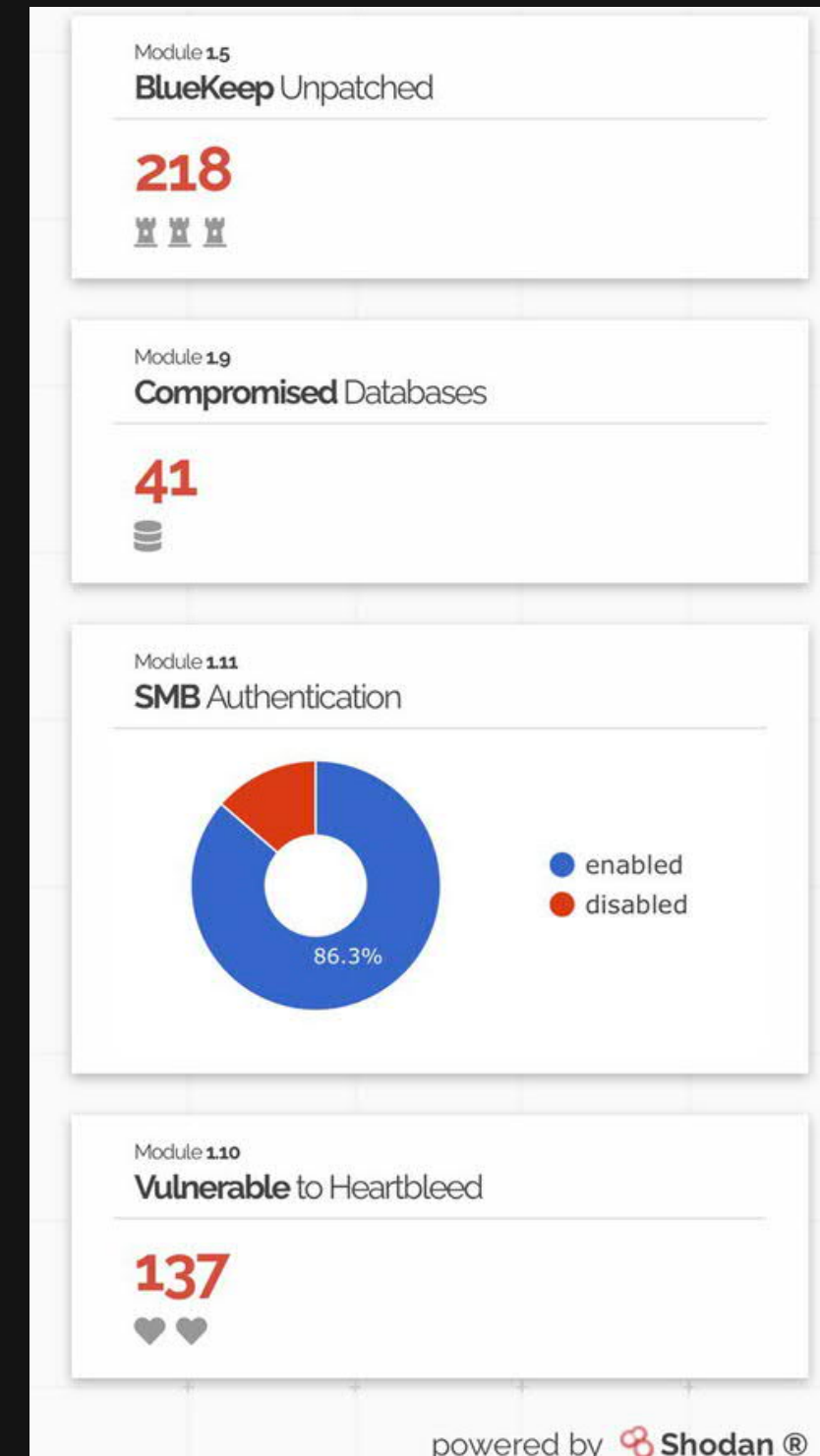
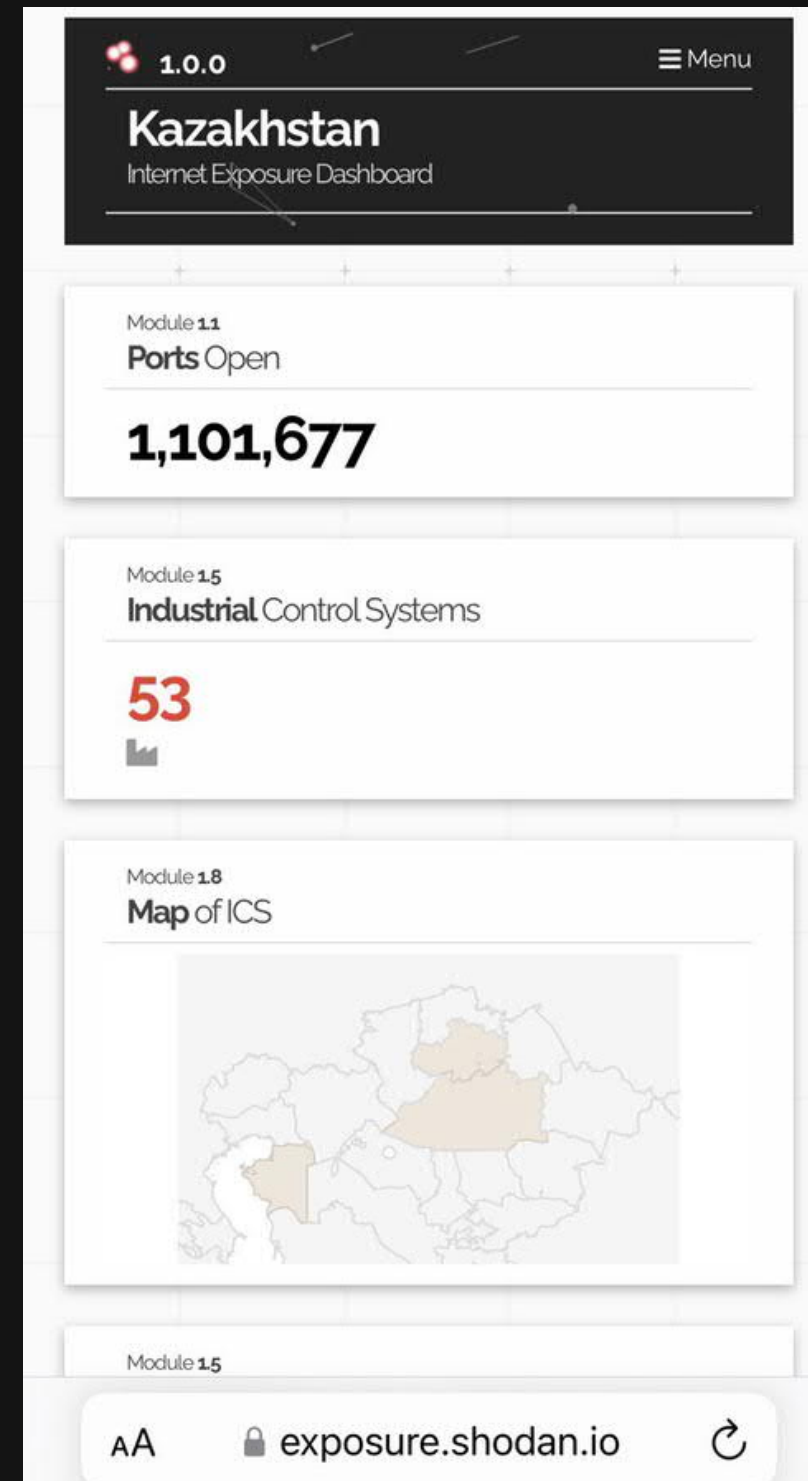
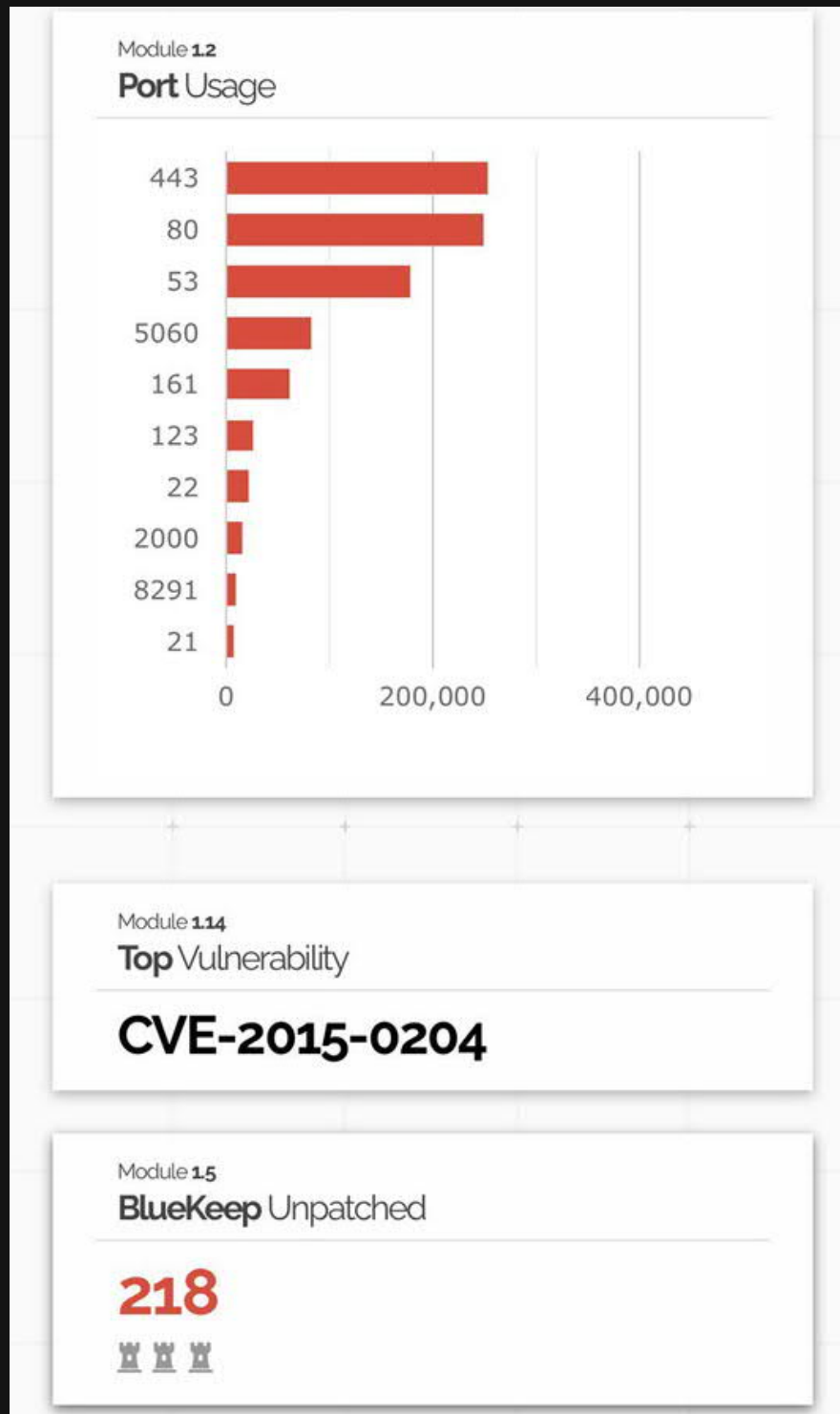
- Безопаснее файрвола
- Уменьшает сервисные затраты (файрволы нужно обслуживать, уязвимости быстро "эксплоитятся")
- Существенно уменьшает риски кибератак

Актуальность применения дата диодов возросла в связи с:

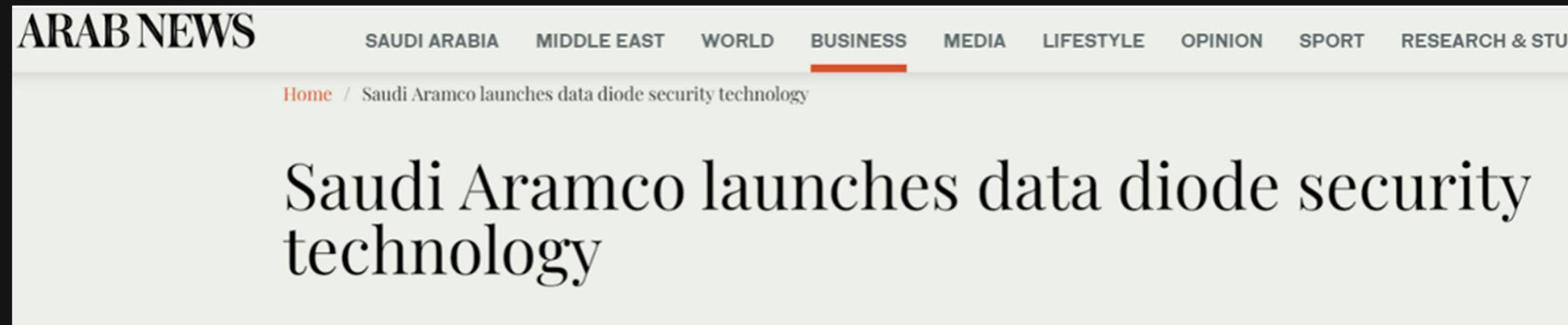
- Требованиями МинЭнерго по передаче данных в ИСУН
- Требованиями Государственной технической службы по передаче данных в ЦОИБ
- Необходимостью взаимодействия производства с головными офисами
- Внедрением программ цифровизации



Все ли защищено в Казахстане?

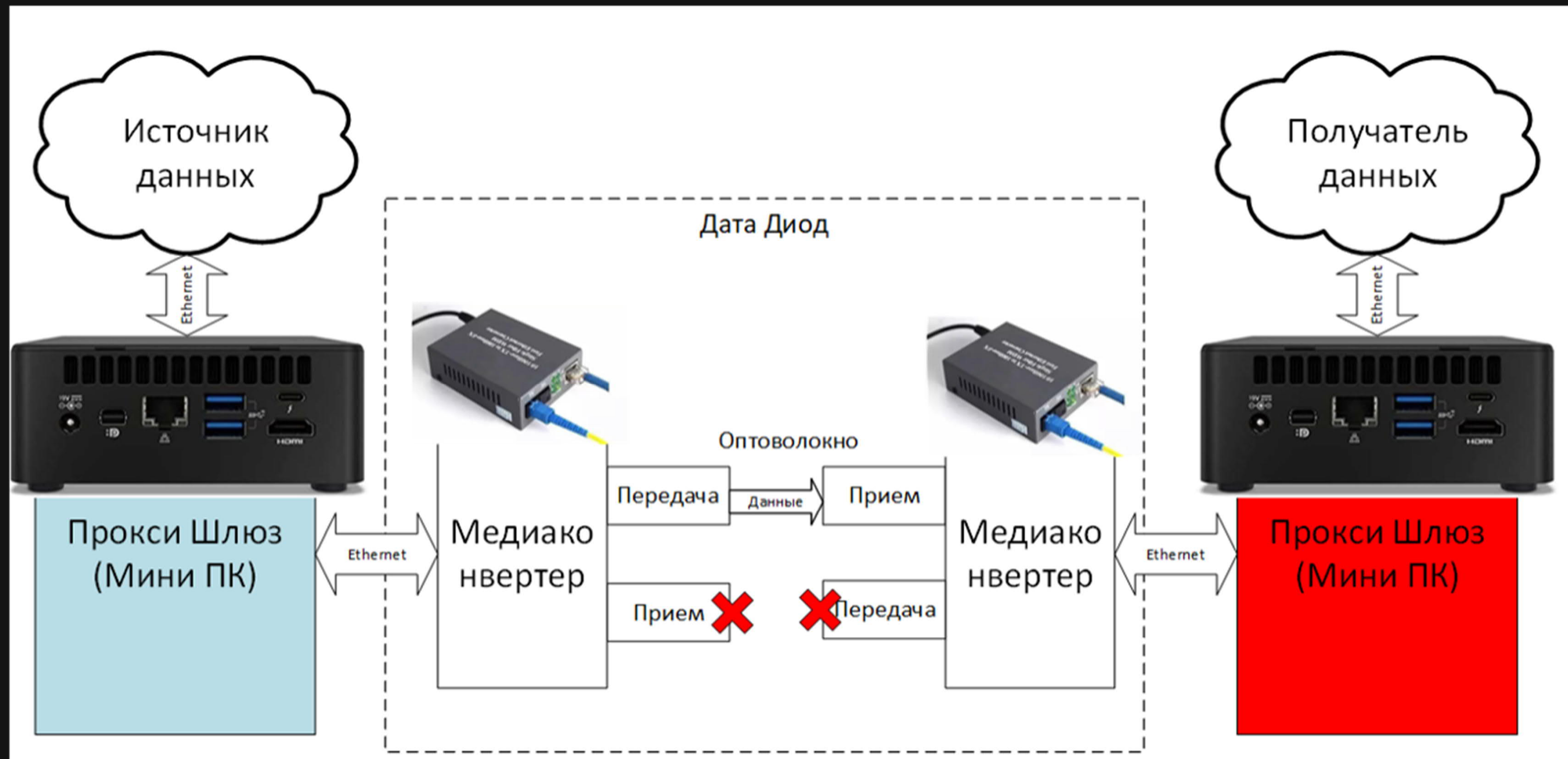


Практика применения

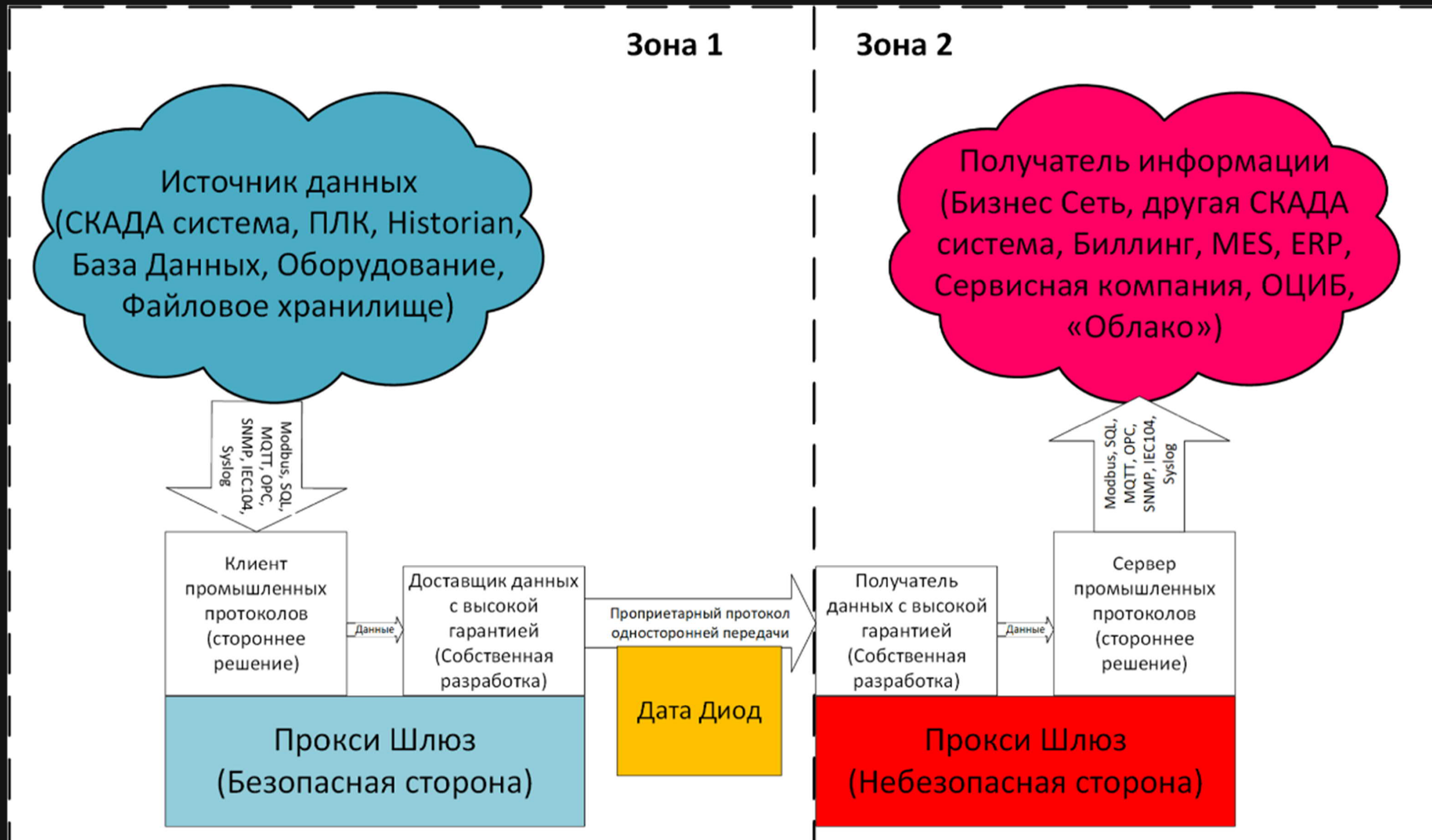


SAUDI ARAMCO		ADNOC		TENGINZCHEVROIL
Aramco решила инвестировать в разработку собственного решения дата диода после разрушительной атаки Trisys\Triton на её ПАЗ систему		Новая стратегия ADNOC по сокращению рисков кибератак, использует дата диоды для ограничения доступа в промышленный сегмент сети		ТШО использует дата диод для передачи энергетической информации в КЕГОК, без предоставления прямого доступа в сеть ТШО

Аппаратная архитектура (MVP)



Логическая схема (MVP)



Программная часть (MVP)

```
main.rs 9 X @rust_panic Cargo.toml config.toml let mut m = Sha1::new(); Untitled-1 ...
src > main.rs > main
61
62     user: &usr,
63     pwd: &cred,
64     options: ConnectionOptions::default(),
65 }?;
66
67 // Execute a one-off query without any parameters.
68 match connection.execute(query: "SELECT * FROM ProcessData", params: ())? {
69     Some(mut cursor: CursorImpl<StatementImpl<'_>>)) => {
70         // Use schema in cursor to initialize a text buffer
71         let mut buffers: ColumnarBuffer<TextColumn<...>> = TextRowSet::for_cursor(BATCH_SIZE, &mut cursor, max_str_limit: Some(4096))?;
72         let mut row_set_cursor: BlockCursor<CursorImpl<StatementImpl<'_>>, ...> = cursor.bind_buffer(row_set_buffer: &mut buffers)?;
73
74         // Iterate over batches
75         while let Some(batch: &&mut ColumnarBuffer<TextColumn<...>>) = row_set_cursor.fetch()? {
76             // Within a batch, iterate over every row
77             for row_index: usize in 0..batch.num_rows() {
78                 let c1: String = String::from_utf8_lossy(batch.at(buffer_index: 0, row_index).unwrap_or(default: &[])).into_owned();
79                 let c2: String = String::from_utf8_lossy(batch.at(buffer_index: 1, row_index).unwrap_or(default: &[])).into_owned();
80
81                 let row_data: TableData = TableData { c1, c2 };
82                 let json_data: String = to_string(&row_data)?;
83                 //sha-1 hash calculation
84                 let hash: String = hex::encode(data: sha1::Sha1::digest(row_data.c2.as_bytes()));
85                 //pushing data over diode
86                 send_data_over_udp(&json_data, &src_addr)?;
87                 //timestamp calculation
88                 let tstamp: DateTime<Local> = Local::now();
89                 //diagnostics output
90                 println!("row {} with c2 hash {} sent at {}", json_data, hash, tstamp);
91             }
92         }
93     }
94     None => {
```


Программная часть (MVP)

```
main.rs 6 x launch.json Cargo.toml
src > main.rs > main
18 socket.set_broadcast(true).unwrap();
19
20 let environment: Environment = Environment::new()?;
21 let mut connection: Connection<'_> = environment.connect(
22     data_source_name: "odbcrust",
23     user: "ddcatcher",
24     pwd: "ddcatcher123",
25     options: ConnectionOptions::default(),
26 );
27
28 loop {
29     match socket.recv_from(&mut buf) {
30         Ok((num_bytes: usize, _src_addr: SocketAddr)) => {
31             let data: &str = std::str::from_utf8(&buf[0..num_bytes])?;
32             let row_data: TableData = serde_json::from_str(&data).unwrap();
33             let id: String = row_data.c1.clone();
34             let v: String = row_data.c2.clone();
35
36             // Insert into database
37             let mut stmt: Result<Prepared<StatementImpl<'>>, ...> = connection.prepare(query:
38                 let params: (&VarCell<Box<[u8]>, Text>, ...) = (&row_data.c2.into_parameter(), &row
39                 stmt?.execute(params);
40             let tstamp: DateTime<Local> = Local::now();
41
42             println!("Received message: {} : {} times: {}", id, v, tstamp);
43         }
44         Err(e: Error) => {
45             eprintln!("Couldn't receive data: {}", e);
46         }
47     }

```

```
PROBLEMS 6 OUTPUT DEBUG CONSOLE TERMINAL
0
Received message: 84 : E01F4D0F-B times: 2023-09-14 12:31:22.220184600 +04:0
0
Received message: 85 : D31562FE-0 times: 2023-09-14 12:31:22.227508700 +04:0
0
Received message: 86 : BC9E1A2C-C times: 2023-09-14 12:31:22.236687400 +04:0
0
Received message: 87 : 6BB32140-3 times: 2023-09-14 12:31:22.242053600 +04:0
0
Received message: 88 : 261BE440-1 times: 2023-09-14 12:31:22.245043900 +04:0
0
Received message: 89 : 0F0418AC-8 times: 2023-09-14 12:31:22.248731400 +04:0
0
Received message: 90 : DD26EE8C-1 times: 2023-09-14 12:31:22.250862500 +04:0
0
Received message: 91 : B926B572-E times: 2023-09-14 12:31:22.260448800 +04:0
0
Received message: 92 : 4CC2EB79-0 times: 2023-09-14 12:31:22.266419400 +04:0
0
Received message: 93 : 16DB1A75-4 times: 2023-09-14 12:31:22.270707100 +04:0
0
Received message: 94 : 9708C1B4-0 times: 2023-09-14 12:31:22.281028100 +04:0
0
Received message: 95 : 1133487E-2 times: 2023-09-14 12:31:22.293192200 +04:0
0
Received message: 96 : 8EE46F05-4 times: 2023-09-14 12:31:22.304003500 +04:0
0
Received message: 97 : C1F01D87-C times: 2023-09-14 12:31:22.323717800 +04:0
0
Received message: 98 : C67DC148-A times: 2023-09-14 12:31:22.338305900 +04:0
0
Received message: 99 : 31870D8B-A times: 2023-09-14 12:31:22.350128800 +04:0
0
Received message: 100 : 2F03A07A-3 times: 2023-09-14 12:31:22.366778200 +04:0

```


Что мы сделаем с грантом?

На средства гранта мы соберем аппаратную часть прототипа

Возможно вы увидите прототип на выставках или в пилотных проектах предприятий страны и зарубежья



Дальнейшее развитие



- Разработка собственного клиента протоколов
- Интеграция дата-диода с существующими продуктами мониторинга и кибербезопасности
- Разработка облачного сервиса сбора и обработки больших данных интегрированного с дата-диодом

Контакты



SALES@AIMI-AUTOMATION.COM

+7 701 444 77 35