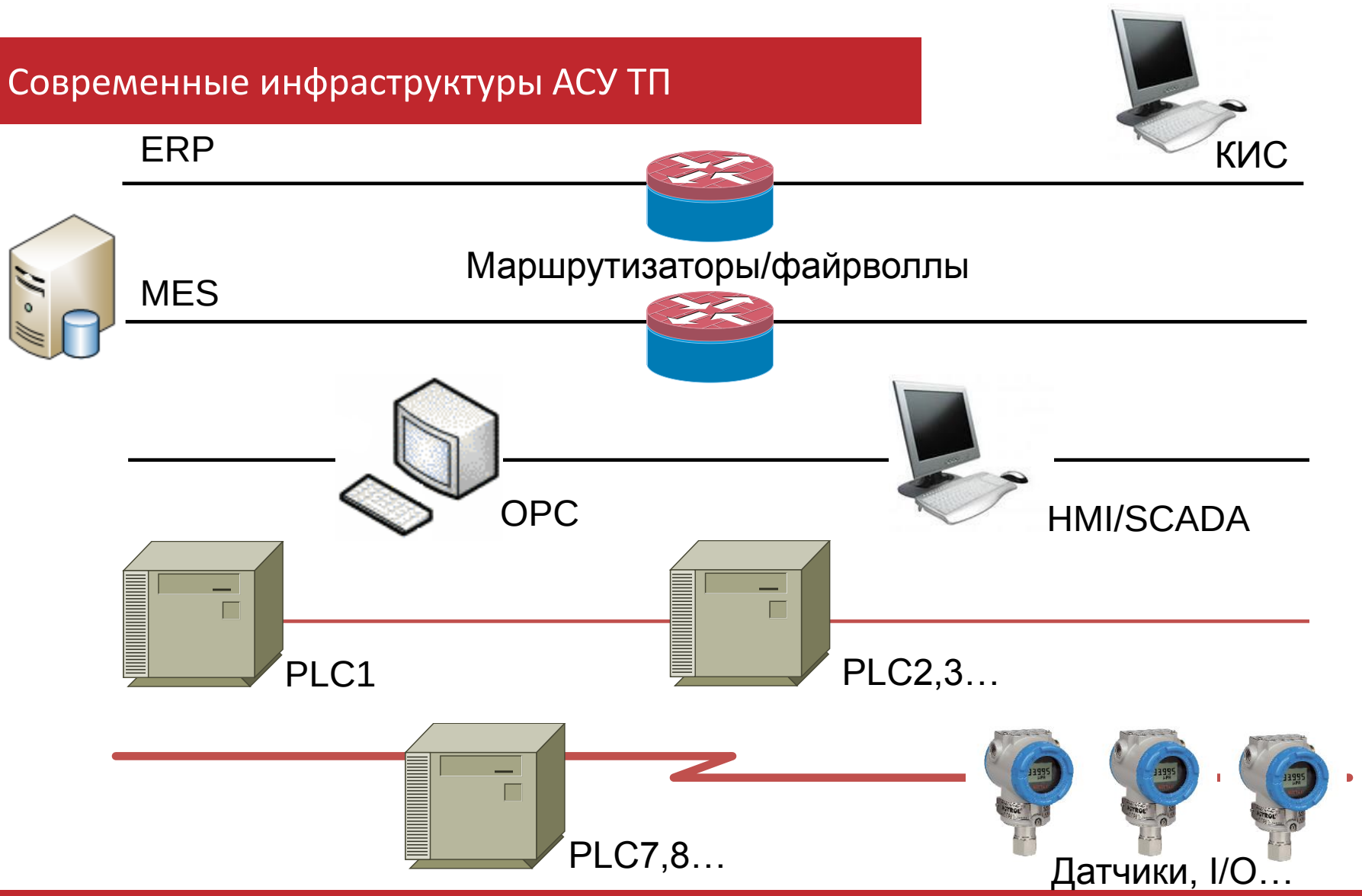
Digital Security

Проблемы безопасности программного обеспечения на нижних уровнях АСУ ТП

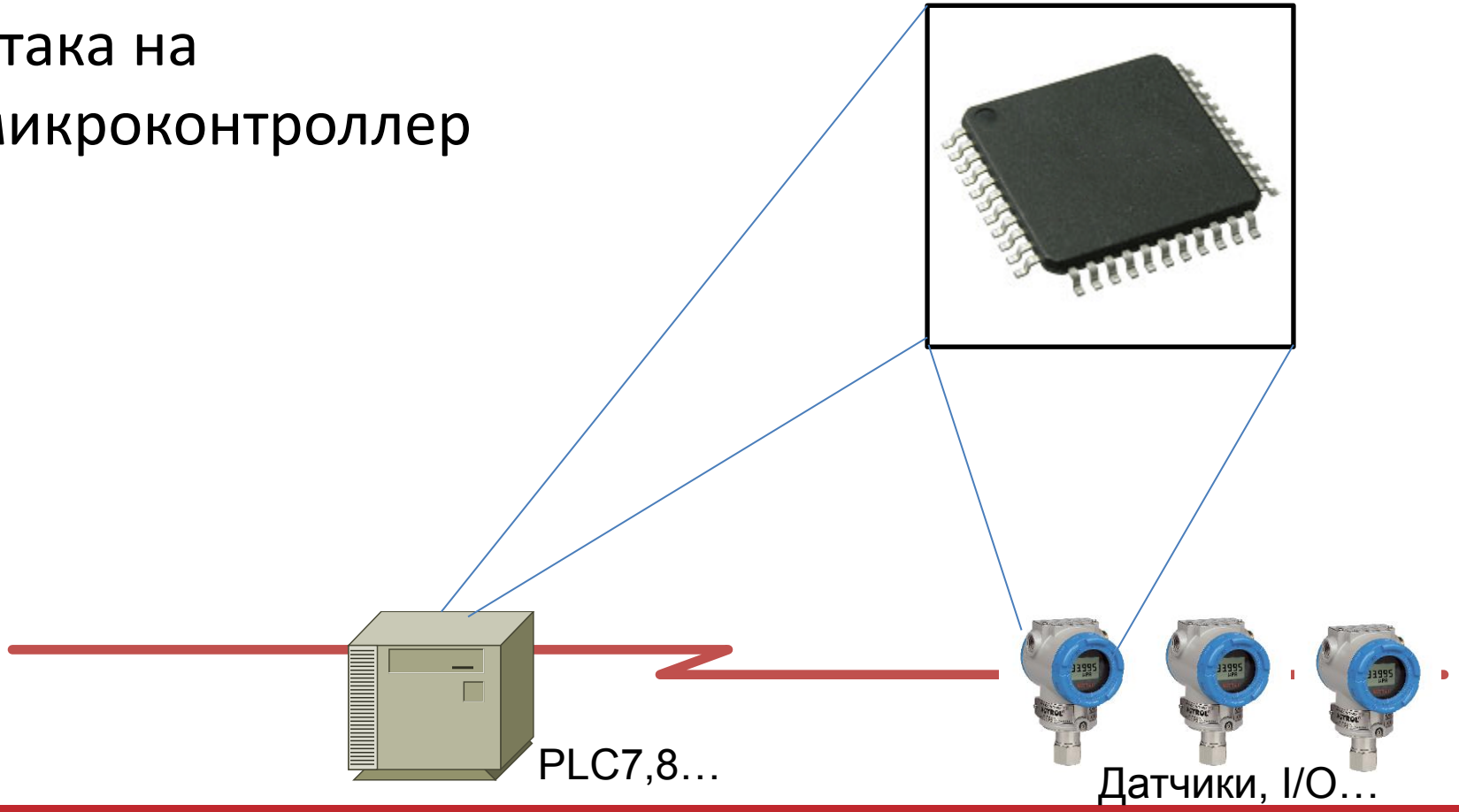
Вадим Бардаков
Аудитор ИБ
Digital Security

Современные инфраструктуры АСУ ТП



Атака на нижний уровень

Атака на микроконтроллер



Как добраться?

- Каналы связи

Как добраться?

- Каналы связи
  - Часто вне охраняемой территории
  - Беспроводные

Как добраться?

- Каналы связи
  - Часто вне охраняемой территории
  - Беспроводные
- Программное обеспечение

Как добраться?

- Каналы связи
  - Часто вне охраняемой территории
  - Беспроводные

- Программное обеспечение
  - Инвазивные атаки
  - Анализ побочных каналов

Как добраться?

- Каналы связи
  - Часто вне охраняемой территории
  - Беспроводные
- Программное обеспечение
  - Инвазивные атаки
  - Анализ побочных каналов

Более чем доступно!

Злоумышленник и устройство

Где уязвимость? Как искать?

- Анализ работы устройства
  - Документация
  - Схемотехника
- Анализ микроконтроллера
  - Документация
  - Порты ввода-вывода
  - Побочные каналы

Злоумышленник и устройство

Где уязвимость? Как искать?

- Анализ работы устройства
  - Документация
  - Схемотехника
- Анализ микроконтроллера
  - Документация
  - Порты ввода-вывода
  - Побочные каналы

Нашел!

Осбенности эксплуатации

Выполнение произвольного кода:

- Неисполняемый стек
- Статичная адресация

Все еще нет доступа к прошивке?

Осбенности эксплуатации

Выполнение произвольного кода:

- Неисполняемый стек
- Статичная адресация

Все еще нет доступа к прошивке?

Выход есть!

Прерывания

- Статичны
- Получают адрес возврата из стека

ROP-friendly

Vector No.	Program Address(2)	Source	Interrupt Definition
1	0x000(1)	RESET	Reset
2	0x001	INT0	Внешнее прерывание 0
3	0x002	INT1	Внешнее прерывание 1
4	0x003	TIMER2 COMP	Совпадение таймера 2
5	0x004	TIMER2 OVF	Переполнение таймера 2
6	0x005	TIMER1 CAPT	Захват таймера 1
7	0x006	TIMER1 COMPA	Совпадение A таймера 1
8	0x007	TIMER1 COMPB	Совпадение B таймера 1
9	0x008	TIMER1 OVF	Переполнение таймера 1
10	0x009	TIMER0 OVF	Переполнение таймера 0
11	0x00A	SPI, STC	SPI завершил передачу
12	0x00B	USART, RXC	Прием по USART завершен
13	0x00C	USART, UDRE	Регистр данных USART пустой
14	0x00D	USART, TXC	Передача по USART завершена
15	0x00E	ADC	АЦП закончил преобразование
16	0x00F	EE_RDY	EEPROM готов
17	0x010	ANA_COMP	Сработал аналоговый компаратор
18	0x011	TWI	Прерывание от TWI
19	0x012	SPM_RDY	Готовность SPM

Конструкции, заложенные компилятором

- Относительно статичны
- Легко использовать

AVR Studio 6.X

Злоумышленник

```
.text:00000049 loc_49:
.text:00000049                 cli
.text:0000004A
.text:0000004A loc_4A:
.text:0000004A                 rjmp    loc_4A
```

Конструкции, заложенные компилятором

- Относительно статичны
- Легко использовать

AVR Studio 6.X

Злоумышленник

```
.text:00000049 loc_49:
.text:00000049                 cli
.text:0000004A
.text:0000004A loc_4A:
.text:0000004A                 rjmp    loc_4A
```

Отказ в обслуживании

Самопрограммирование

- Передать управление на загрузчик в обход проверок
- Загрузить код через прерывания

17.5 Page Size

Table 17-5. No. of Words in a Page and No. of Pages in the Flash

Flash Size	Page Size	PCWORD	No. of Pages	PCPAGE	PCMSB
512 words (1K byte)	16 words	PC[3:0]	32	PC[8:4]	8

Самопрограммирование

- Передать управление на загрузчик, в обход проверок
- Загрузить код через прерывания

17.5 Page Size

Table 17-5. No. of Words in a Page and No. of Pages in the Flash

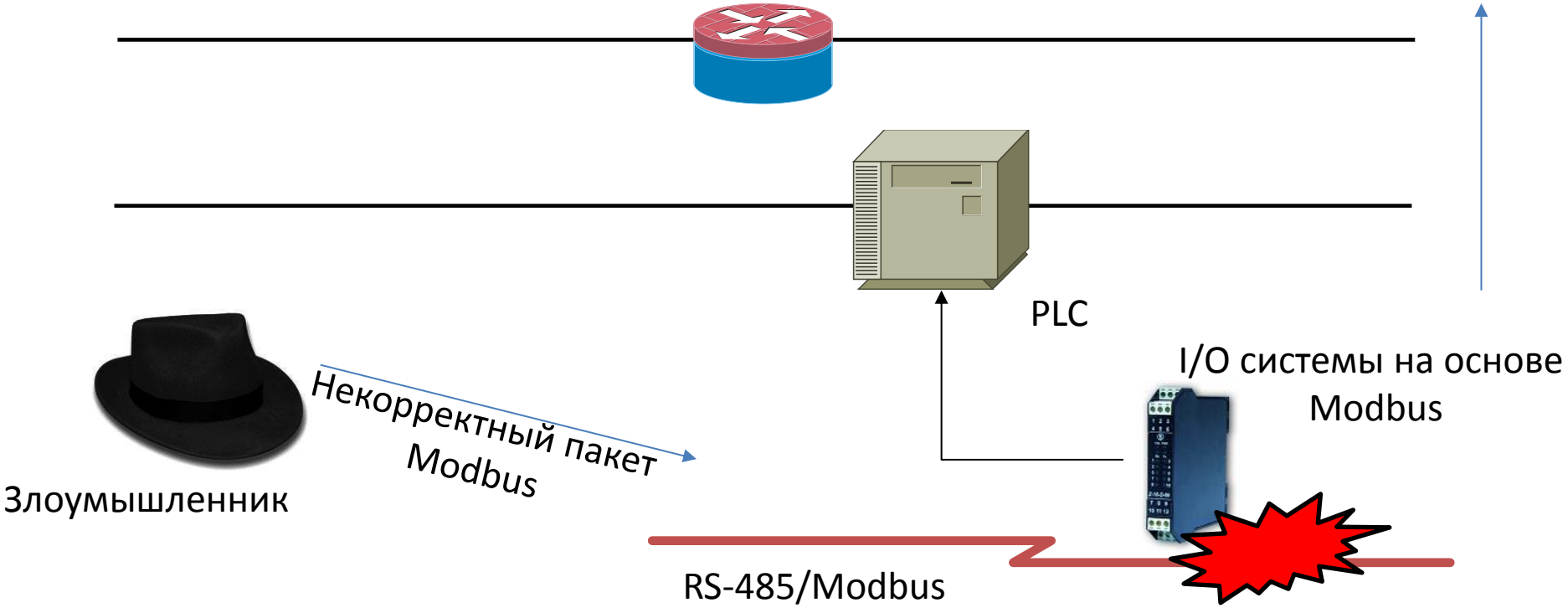
Flash Size	Page Size	PCWORD	No. of Pages	PCPAGE	PCMSB
512 words (1K byte)	16 words	PC[3:0]	32	PC[8:4]	8

Модификация функций устройства!
Получение полного контроля!

Две основные проблемы

- Аппаратная защита замедляет скорость реагирования устройства:
  - Программный ALSR
  - Рандомизация при компиляции
- Аудит кода? Функциональные тесты

В итоге



Вывод

- Атаки могут быть проведены «вслепую»
- Последствия различны:
  - DoS
  - Несанкционированный мониторинг системы
  - Изменение конфигурации устройств
  - и т. д.
- Защита только на стадии проектирования

Digital Security

Digital Security в Москве: (495) 223-07-86
Digital Security в Санкт-Петербурге: (812) 703-15-47

v.bardakov@dsec.ru