РусКрипто'2018

XX юбилейная международная научно-практическая конференция, посвященная актуальным вопросам криптографии и информационной безопасности

Методика разработки защищенных систем, содержащих встроенные устройства

Чечулин Андрей[1,2], Левшун Дмитрий[2,3]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
[3] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

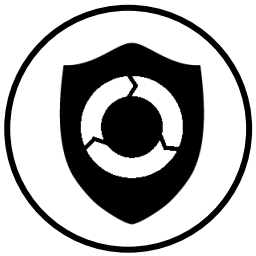
Солнечногорск, 22 марта, 2018

Содержание

- Анализ существующих решений
- Подход к проектированию
- Применение подхода
- Область применения
- Заключение
- Контакты

Анализ существующих решений

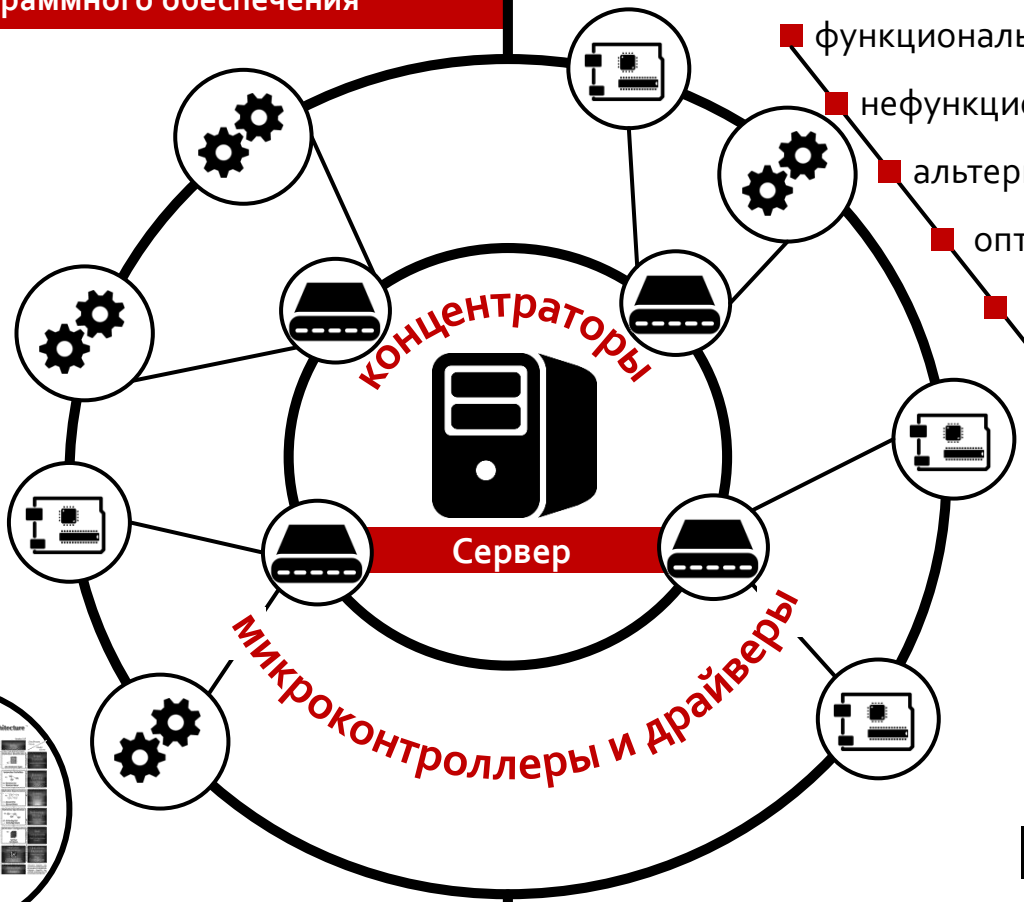
Безопасность программного обеспечения



Microsoft SDL

Cisco SDL

Zachman



- функциональные требования
- нефункциональные требования
- альтернативы
- оптимальный набор
- статическое тестирование

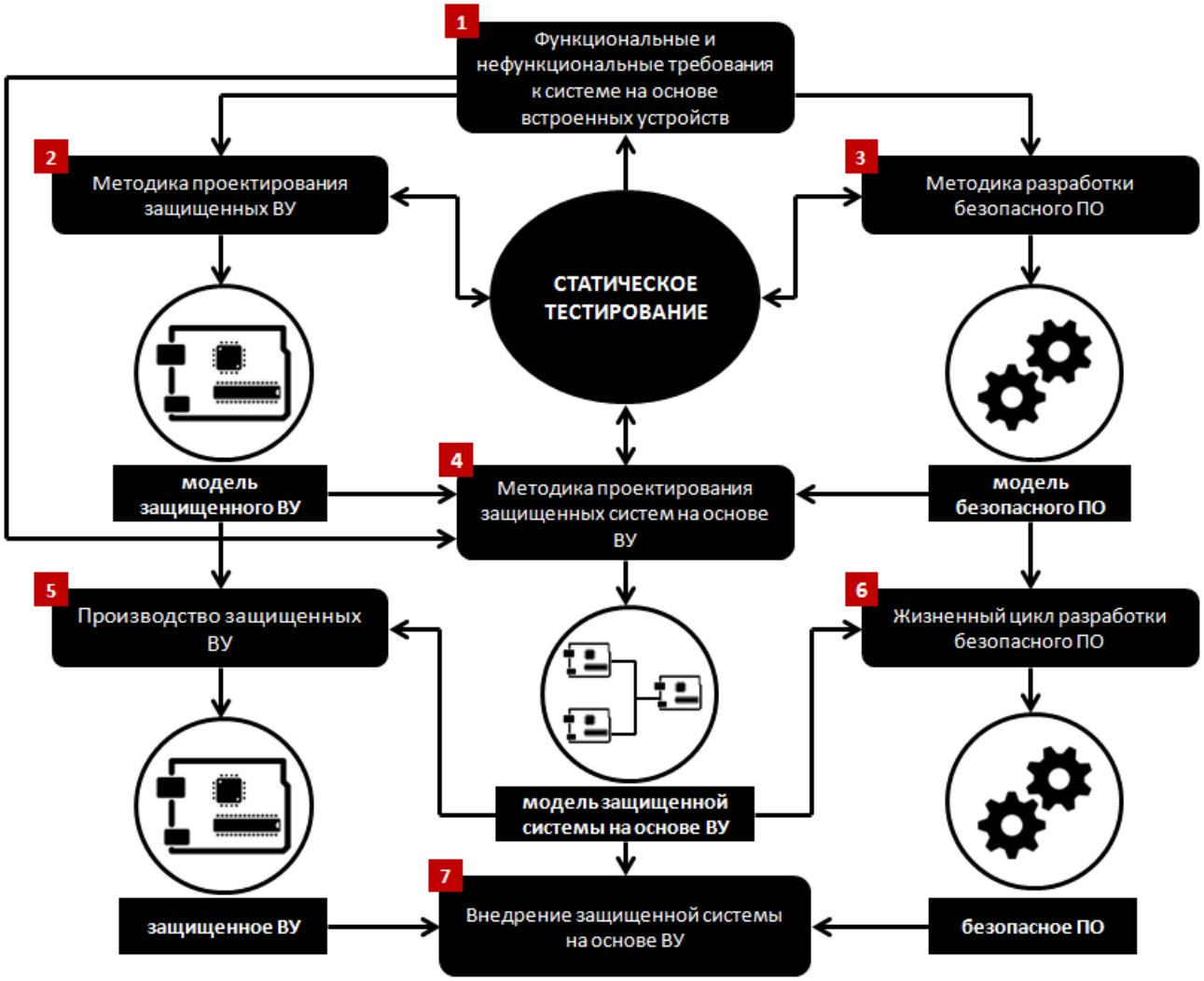
Подход к проектированию защищенных встроенных устройств

SecFutur

Проект SecFutur

Безопасность аппаратного обеспечения

Подход к проектированию (1/8)



Подход к проектированию (2/8)

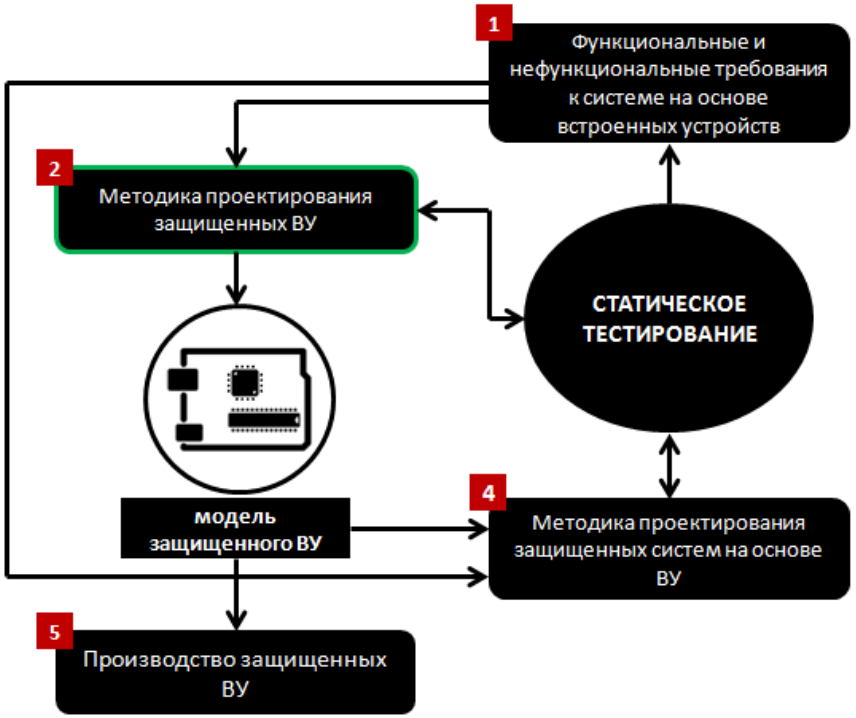
Функциональные требования:

- Требования к встроенным устройствам системы (от **шага 1** на **шаг 2**)
- Требования к программному обеспечению системы (от **шага 1** на **шаг 3**)
- Требования к среде передачи данных системы (от **шага 1** на **шаги 2-4**)

Нефункциональные требования:

- Допустимый диапазон цены, энергопотребления и размера встроенных устройств (от **шага 1** на **шаг 2**)
- Допустимый диапазон цены и ресурсопотребления программного обеспечения (от **шага 1** на **шаг 3**)

Подход к проектированию (3/8)



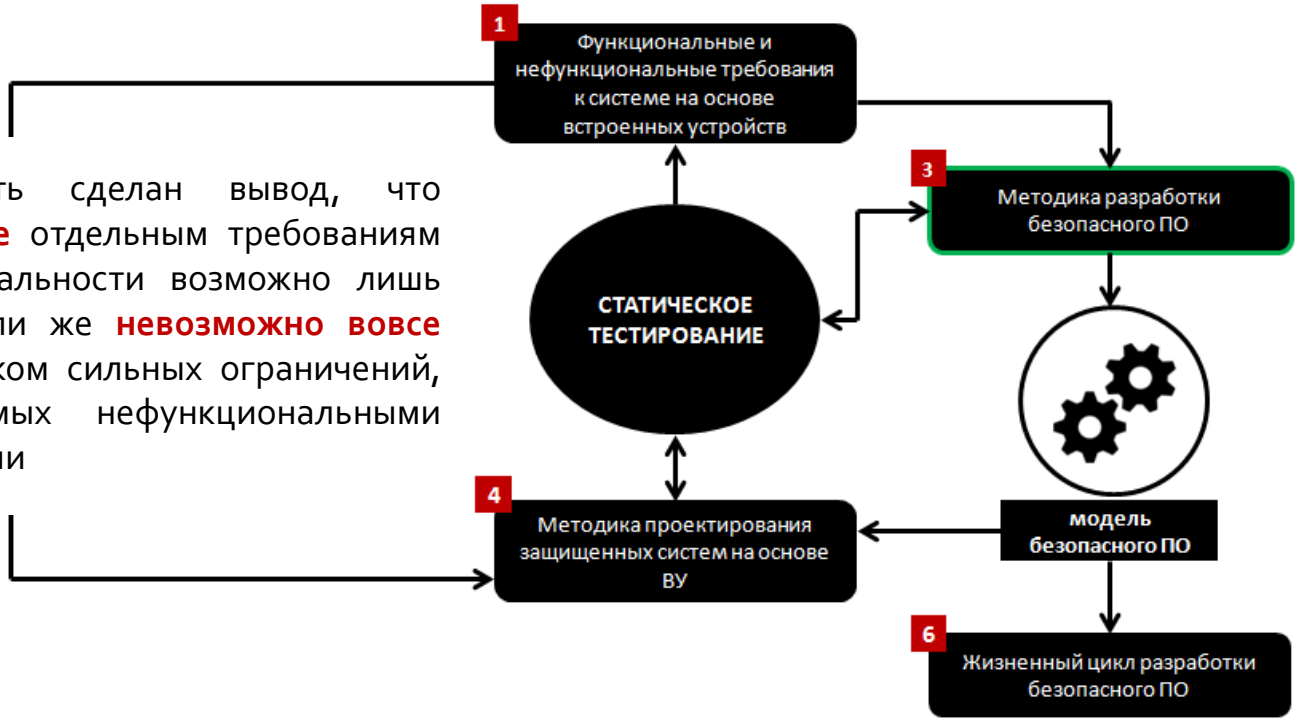
- Может быть сделан вывод, что **соответствие** отдельным требованиям к функциональности возможно лишь **частично** или же **невозможно вовсе** ввиду слишком сильных ограничений, накладываемых нефункциональными требованиями

Методика:

- **Выявление** перечня **возможных альтернатив** компонентного состава встроенных устройств
- **Проверка** полученных альтернатив **на соответствие** нефункциональным требованиями
- **Выбор** оптимальной **альтернативы** среди возможных с точки зрения нефункциональных требований
- **Статическое тестирование:** перечень возможных **вредоносных воздействий** на модель анализируемого встроенного устройства

Подход к проектированию (4/8)

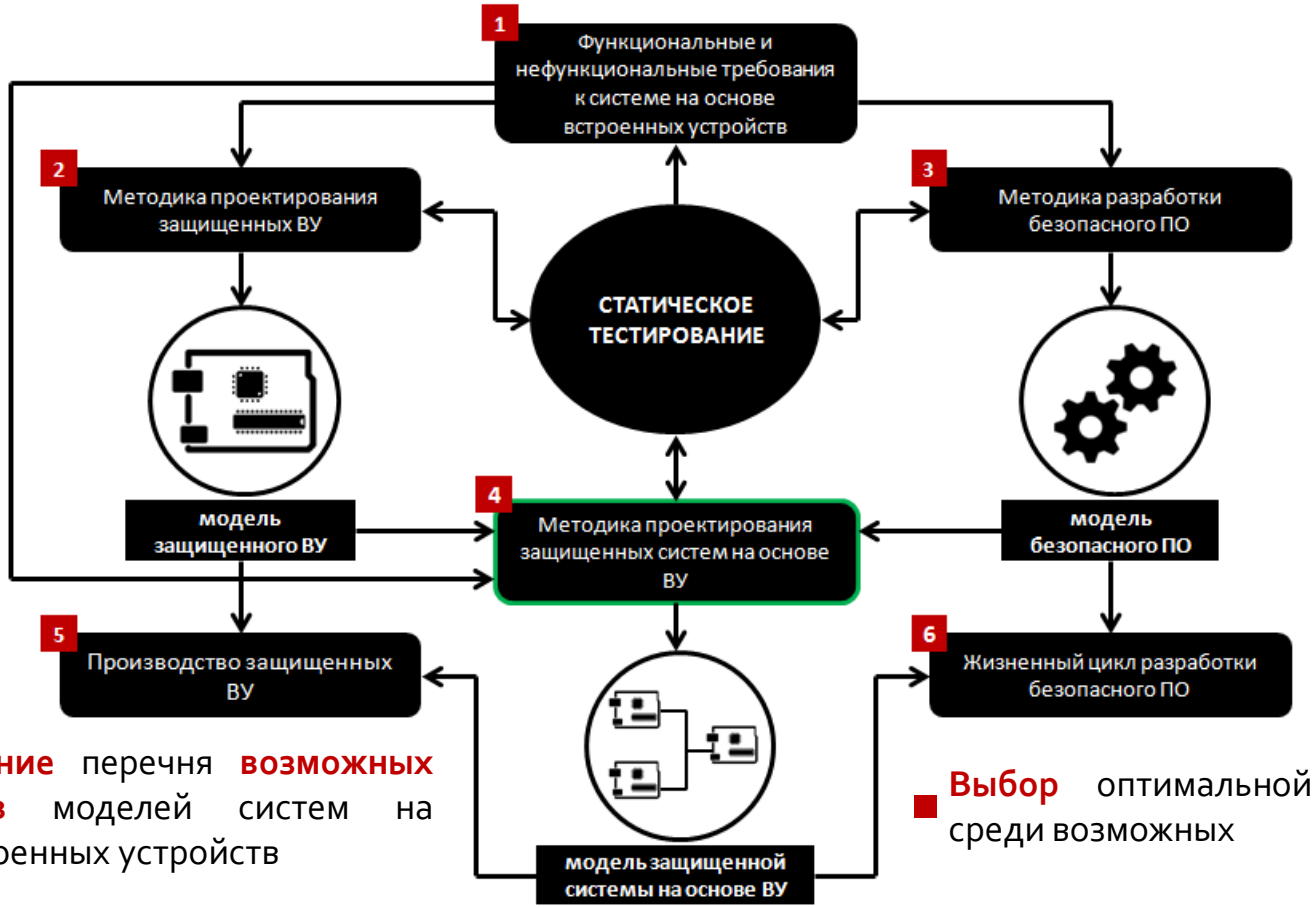
Может быть сделан вывод, что **соответствие** отдельным требованиям к функциональности возможно лишь **частично** или же **невозможно вовсе** ввиду слишком сильных ограничений, накладываемых нефункциональными требованиями



Методика:

- **Анализ** требований к **безопасности** и **архитектуре** программного обеспечения системы
- **Статическое тестирование** на основе **оценки рисков** и **модели угроз**

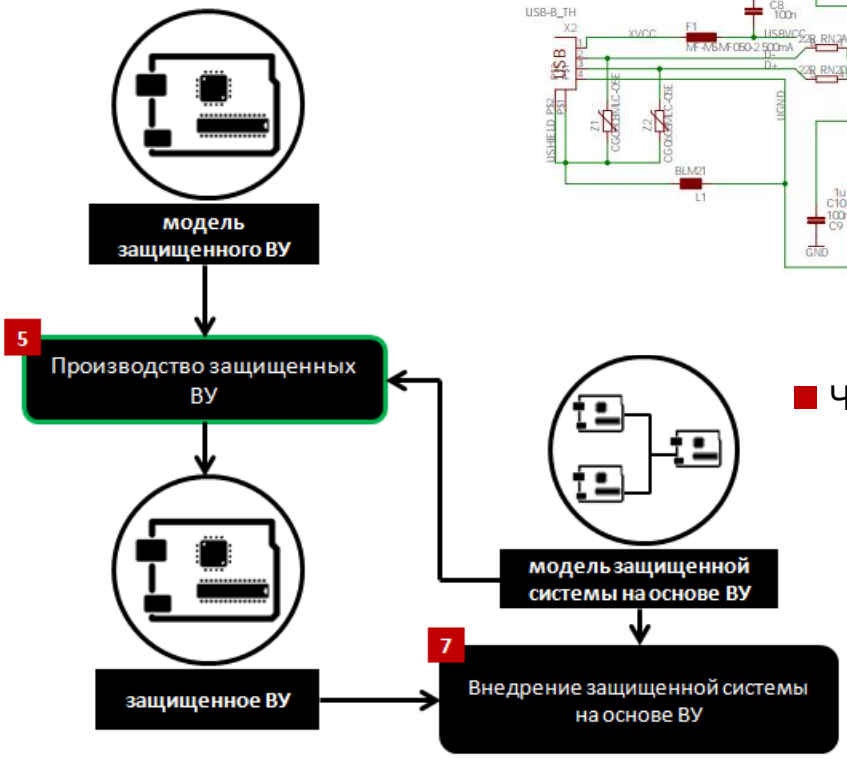
Подход к проектированию (5/8)

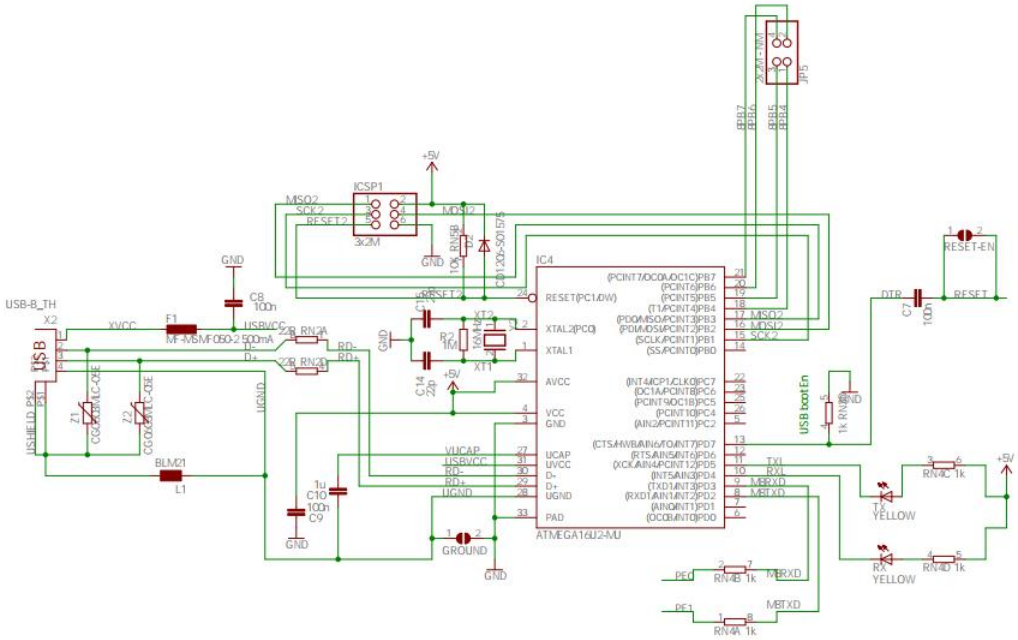


Методика:

- **Формирование** перечня **возможных альтернатив** моделей систем на основе встроенных устройств
- **Проверка** соответствия полученных **альтернатив** нефункциональным требованиям
- **Выбор** оптимальной **альтернативы** среди возможных
- **Статическое тестирование:** анализ перечня возможных вредоносных воздействий

Подход к проектированию (6/8)





- Часть схемы **Arduino Mega 2560**

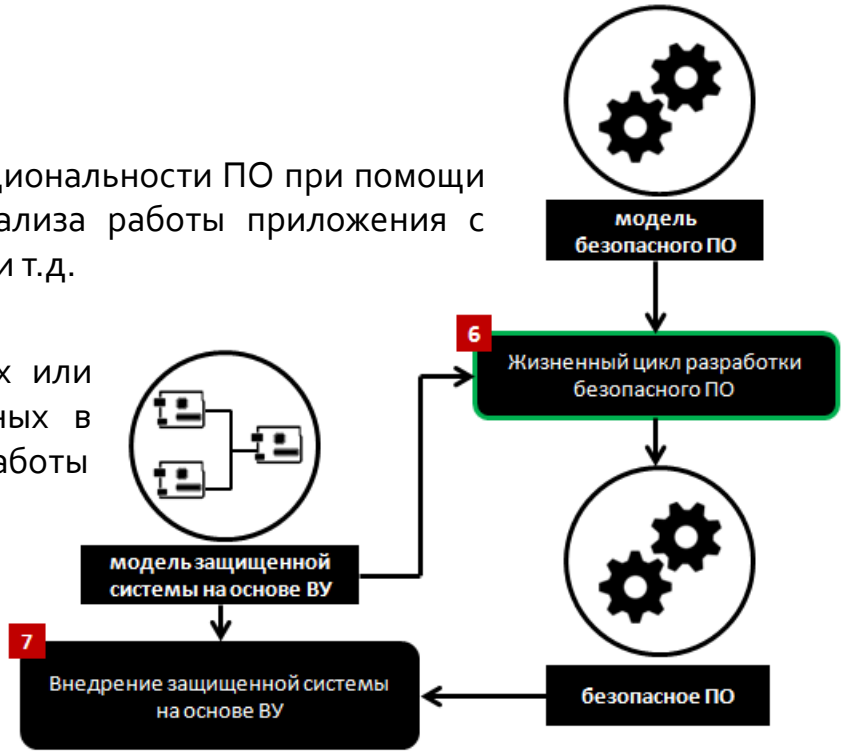
Подход к проектированию (7/8)

Внедрение:

- **Блокировка небезопасных функций:** анализ всех вызовов функций и API в исходном коде и запрет использования тех, которые признаны небезопасными
- **Статическое тестирование:** проверка исходного кода на соответствие политике безопасности

Верификация:

- **Динамический анализ**: проверка функциональности ПО при помощи инструментов для поведенческого анализа работы приложения с памятью, привилегиями пользователей и т.д.
- **Фаззинг:** отправка заведомо неверных или случайных данных в качестве исходных в приложение с целью прекращения его работы
- **Анализ векторов атак:** пересмотр перечня возможных векторов атак и моделей угроз после любых изменений, внесенных в программное обеспечение или систему



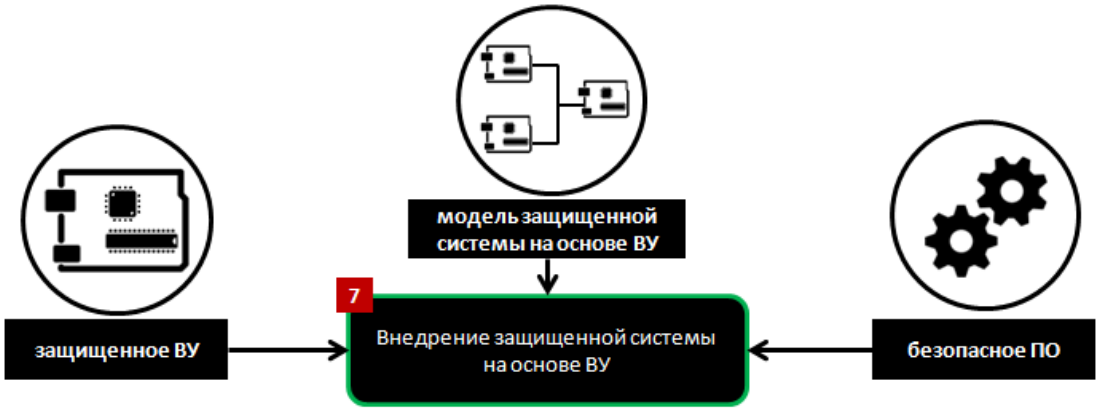
Подход к проектированию (8/8)

Внедрение:

- Размещение **встроенных устройств**, прокладка линий связи между ними, а также их настройка
- Установка и настройка **программного обеспечения**, а также связанных с ним механизмов защиты
- Результат: **готовая к использованию** защищенная система на основе встроенных устройств

Защищенность системы обусловлена:

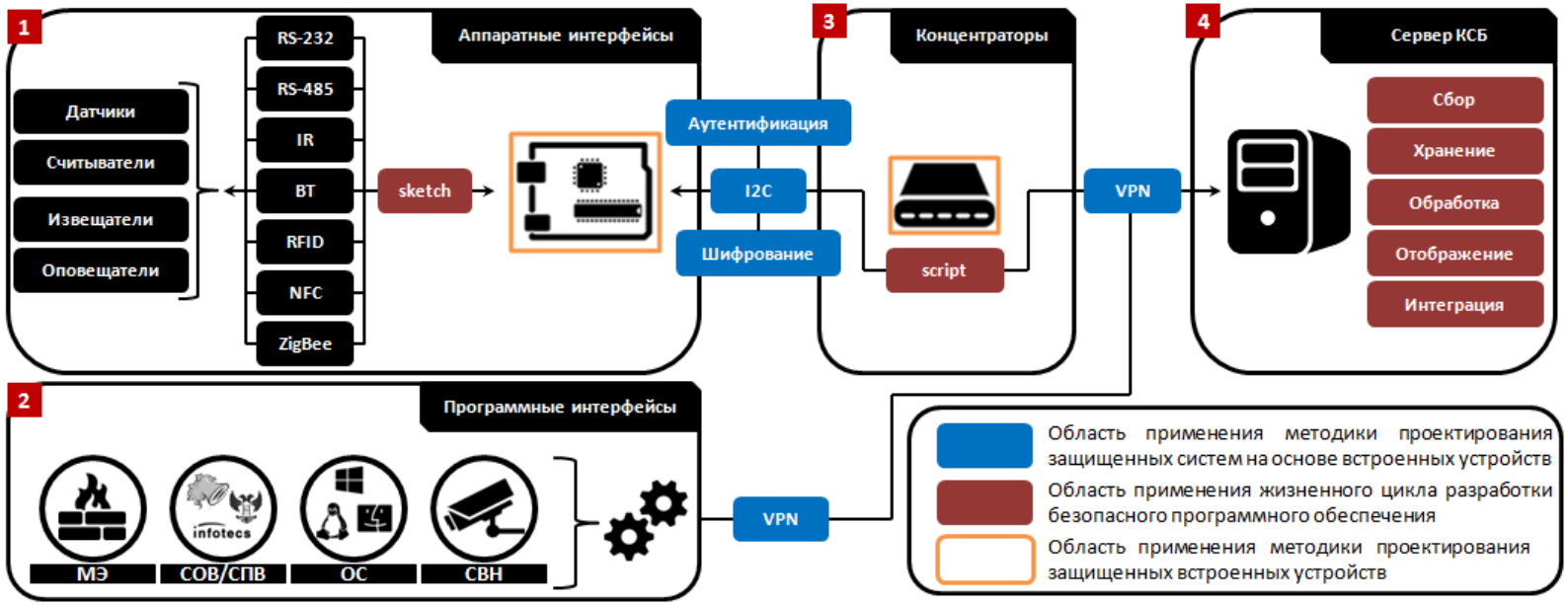
- методикой проектирования защищенных **встроенных устройств** на уровне моделей встроенных устройств
- методикой разработки защищенного **программного обеспечения** на уровне моделей программного обеспечения
- методикой проектирования защищенных **систем на основе встроенных устройств** на уровне модели системы
- жизненным циклом разработки защищенного **программного обеспечения** на этапе разработки программного обеспечения



Применение подхода (1/8)

Исходные данные:

- Система на основе встроенных устройств, которая состоит из четырёх основных модулей: аппаратных интерфейсов (**модуль 1**), программные интерфейсы (**модуль 2**), концентраторы (**модуль 3**), сервер комплексной системы безопасности (**модуль 4**)



Цель:

- Применение разработанного подхода для разработки **защищенной** комплексной системы безопасности на основе встроенных устройств

Применение подхода (2/8)

Шаг 1: функциональные и нефункциональные требования к системе на основе встроенных устройств

- Функциональные и нефункциональные требования к системе на основе встроенных устройств могут быть разделены на **требования к встроенным устройствам**, **требования к программному обеспечению**, и **требования к среде передачи данных** системы

Таблица 1. Функциональные требования к аппаратным интерфейсам

требования	N	описание
к аппаратному обеспечению	1	Обеспечение взаимодействия с проводными и беспроводными извещателями, оповещателями и датчиками
	2	Обеспечение взаимодействия с внешними электронными компонентами систем физической безопасности: считывателями, устройствами вывода текстовой и звуковой информации, звуковых и световых сигналов
	3	Обеспечение передачи данных через структурированную кабельную сеть
	4	Обеспечение возможности автономного функционирования на период отсутствия электроснабжения не превышающий 24 часа
к программному обеспечению	5	Обеспечение возможности локального хранения журнальных записей
	6	Шифрование передаваемых данных

Применение подхода (3/8)

Шаг 1: функциональные и нефункциональные требования к системе на основе встроенных устройств

Таблица 2. Функциональные требования к концентраторам

требования	N	описания
к аппаратному обеспечению	1	Обеспечение взаимодействия с внешними электронными компонентами: устройствами вывода текстовой информации, звуковых и световых сигналов
	2	Обеспечение взаимодействия по беспроводному каналу передачи данных
	3	Обеспечение передачи данных посредством Ethernet
	4	Обеспечение возможности автономного функционирования на период отсутствия электроснабжения, не превышающий 24 часа
к программному обеспечению	5	Обеспечение передачи данных посредством HTTP, HTTPS, SOAP
	6	Обеспечение возможности запуска приложений на языках Java, Python и C++
	7	Обеспечение безопасного хранения журнальных записей
	8	Обеспечение шифрования передаваемых данных
	9	Обеспечение возможности настройки и управления посредством веб-панели при локальном Ethernet подключении

Применение подхода (4/8)

Шаг 1: функциональные и нефункциональные требования к системе на основе встроенных устройств

Таблица 3. Нефункциональные требования к аппаратным интерфейсам

требования	описание
энергоэффективность	Обеспечение возможности автономного функционирования на период отсутствия электроснабжения, не превышающий 24 часа
цена	Минимизация стоимости микроконтроллера, его расширений, адаптеров и периферийных устройств, необходимых для соответствия функциональным требованиям
размер	Минимизация размера микроконтроллера, его расширений, адаптеров и периферийных устройств, чтобы толщина аппаратных интерфейсов не превышала 3 см

Таблица 4. Нефункциональные требования к концентраторам

требования	описание
энергоэффективность	Обеспечение возможности автономного функционирования на период отсутствия электроснабжения, не превышающий 24 часа
цена	Минимизация стоимости микроконтроллера, его расширений, адаптеров и периферийных устройств, необходимых для соответствия функциональным требованиям
размер	Минимизация размера микроконтроллера, его расширений, адаптеров и периферийных устройств, чтобы толщина концентратора не превышала 5 см

Применение подхода (5/8)

Шаг 1: функциональные и нефункциональные требования к системе на основе встроенных устройств

Таблица 5. Функциональные требования к программному обеспечению

требования	описание
к архитектуре	Обеспечение возможности расширения системы посредством внедрения новых устройств и компонентов (**масштабируемость**)
	Обеспечение возможности независимой разработки и тестирования элементов системы в зависимости от их функциональности (**модульность**)
	Обеспечение возможности сохранения работоспособности системы при выходе из строя одного или нескольких её компонентов (за исключением работоспособности самого компонента) (**отказоустойчивость**)
к исходному коду	Обеспечение возможности использования скомпилированных исходных кодов на различных аппаратных платформах или операционных системах при условии замены вызовов только специфичных функций (**кроссплатформенность**)
	Обеспечение возможности независимой разработки и тестирования элементов программного обеспечения в зависимости от их функциональности (**модульность**)
к среде передачи данных	Обеспечение возможности динамической адресации устройств системы
	Обеспечение возможности аутентификации и шифрования передаваемых данных
	Обеспечение возможности передачи сообщений размером 128 байт

Применение подхода (6/8)

Шаг 2: методика проектирования защищенных встроенных устройств

Таблица 6. Результаты 2^ого шага

встроенное устройство	описание
аппаратный интерфейс	Arduino Mega 2560, адаптер, 12 мА DC 5 В 12 мм Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 10000 мАч, стоимостью 2700 рублей и энергопотреблением 379 мАч
концентратор	Raspberry Pi 3, 8 GB microSD, DC 5 В Character LCD 16x2, 12 мА DC 5 В 12 мм Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 20000 мАч, стоимостью 5300рублей и энергопотреблением 824 мАч

Шаг 3: методика проектирования безопасного программного обеспечения

Таблица 7. Результаты 3^его шага

программное обеспечение	описание
база данных	PostgreSQL, распределенная, с резервным копированием
сервер	Tomcat, фреймворк Spring Security, HTTPS, OpenVPN
программный интерфейс	Java, C++, Windows, Unix, MacOS, OpenVPN
скрипты, прошивка концентратора	Python, Wiring, Raspbian, OpenVPN
прошивка аппаратного интерфейса	Wiring, расширенный I2C с адресацией, аутентификацией и шифрованием

Применение подхода (7/8)

Шаг 4: методика проектирования защищенных систем на основе встроенных устройств

Таблица 8. Результаты 4ого шага. Часть 1

элемент	часть	описание
аппаратный интерфейс	аппаратное обеспечение	Arduino Mega 2560, адаптер, 12 мА DC 5 В 12 мм Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 10000 мАч, стоимостью 2700 рублей и энергопотреблением 379 мАч
	прошивка	Wiring, модульность, расширяемость
	протокол	Wiring, расширенный I2C с адресацией, аутентификацией и шифрованием
программный интерфейс	ОС	Windows, Unix, MacOS
	исходный код	Java, C++, модульность, масштабируемость
	протокол	OpenVPN
концентратор	аппаратное обеспечение	Raspberry Pi 3, 8 GB microSD, DC 5 В Character LCD 16x2, 12 мА DC 5 В 12 мм Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 20000 мАч, стоимостью 5300рублей и энергопотреблением 824 мАч
	скрипты	Python, Java
	база данных	PostgreSQL
	протокол	расширенный Serial с аутентификацией и шифрованием, OpenVPN

Применение подхода (8/8)

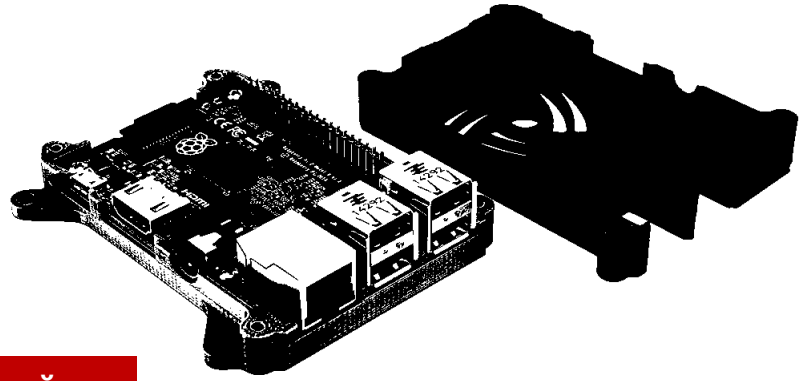
Шаг 4: методика проектирования защищенных систем на основе встроенных устройств

Таблица 9. Результаты 4ого шага. Часть 2

элемент	часть	описание
сервер	контейнер сервлетов	Tomcat
	фреймворк	Spring Security
	база данных	PostgreSQL, распределенная, с резервным копированием
	протокол	OpenVPN, HTTPS

Шаг 5: производство встроенных устройств

- Производство микроконтроллеров, 3D печать



Шаг 6: Жизненный цикл разработки безопасного ПО

- Разработка в соответствии с Microsoft SDL

Шаг 7: Внедрение защищенной системы на основе встроенных устройств

- Размещение и настройка встроенных устройств, прокладка линий связи между ними; установка и настройка программного обеспечения, а также соответствующих защитных механизмов.

Область применения

- Подход позволяет разработчикам проектировать **сложные защищенные системы** на основе встроенных устройств без привлечения **эксперта**
- Перечень возможных **альтернатив** зависит от качества **базы знаний**
- **Эксперт** выберет альтернативы на **качественно более высоком** уровне
- Подход может быть **полезен** эксперту в качестве инструмента для **автоматизации** отдельных **рутинных** задач
- Подход может быть **полезен** эксперту как **источник решений**, отличных от его **субъективных предпочтений**

Заключение

Заключение:

- Разработанный подход представляет собой **объединение** подхода к разработке **безопасного программного обеспечения**, методики проектирования **защищенных встроенных устройств**, а также разработанной методики проектирования **защищенной системы на основе встроенных устройств**.
- **Корректность** разработанного подхода **подтверждается** его применением при разработке комплексной системы киберфизической безопасности на основе встроенных устройств

Дальнейшие исследования:

- Проведение дополнительных экспериментов по применению разработанного подхода к проектированию защищенных систем на основе встроенных устройств
- Расширение уже существующей базы знаний по компонентному составу встроенных устройств, поддерживаемым интерфейсам и протоколам передачи данных
- Применение базы данных уязвимостей для повышения эффективности процесса статического тестирования

Контакты

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича:

- Почтовый адрес: 193232, Санкт-Петербург, пр. Большевиков д.22, к.1
- Телефон: +7 (812) 326-31-50
- URL: http://www.sut.ru/

Лаборатория проблем компьютерной безопасности ФГБУН СПИИРАН:

- Почтовый адрес: 199178, Санкт-Петербург, 14-я линия В.О., д.39
- Телефон: +7(812)328-26-42
- Факс: +7(812)328-44-50
- URL: http://comsec.spb.ru

Международная лаборатория информационной безопасности киберфизических систем Университета ИТМО:

- Почтовый адрес : 191002 , Санкт-Петербург, Ломоносова д. 9

Авторы:

- Чечулин Андрей, chechulin@comsec.spb.ru, http://comsec.spb.ru/chechulin
- Левшун Дмитрий, levshun@comsec.spb.ru, http://comsec.spb.ru/levshun

Работа выполнена при поддержке Гранта президента Российской Федерации (МК-314.2017.9).