Система «Домашняя сеть»

В данной презентации моя домашняя сеть рассматривается с точки зрения информационной безопасности.

Целостность
(Сильно выражено)

Моя домашняя сеть отделена от глобальной сети Интернет по границам 2 видов: кабель от маршрутизатора к провайдеру и каналы связи между мобильными устройствами и сотовой вышкой.

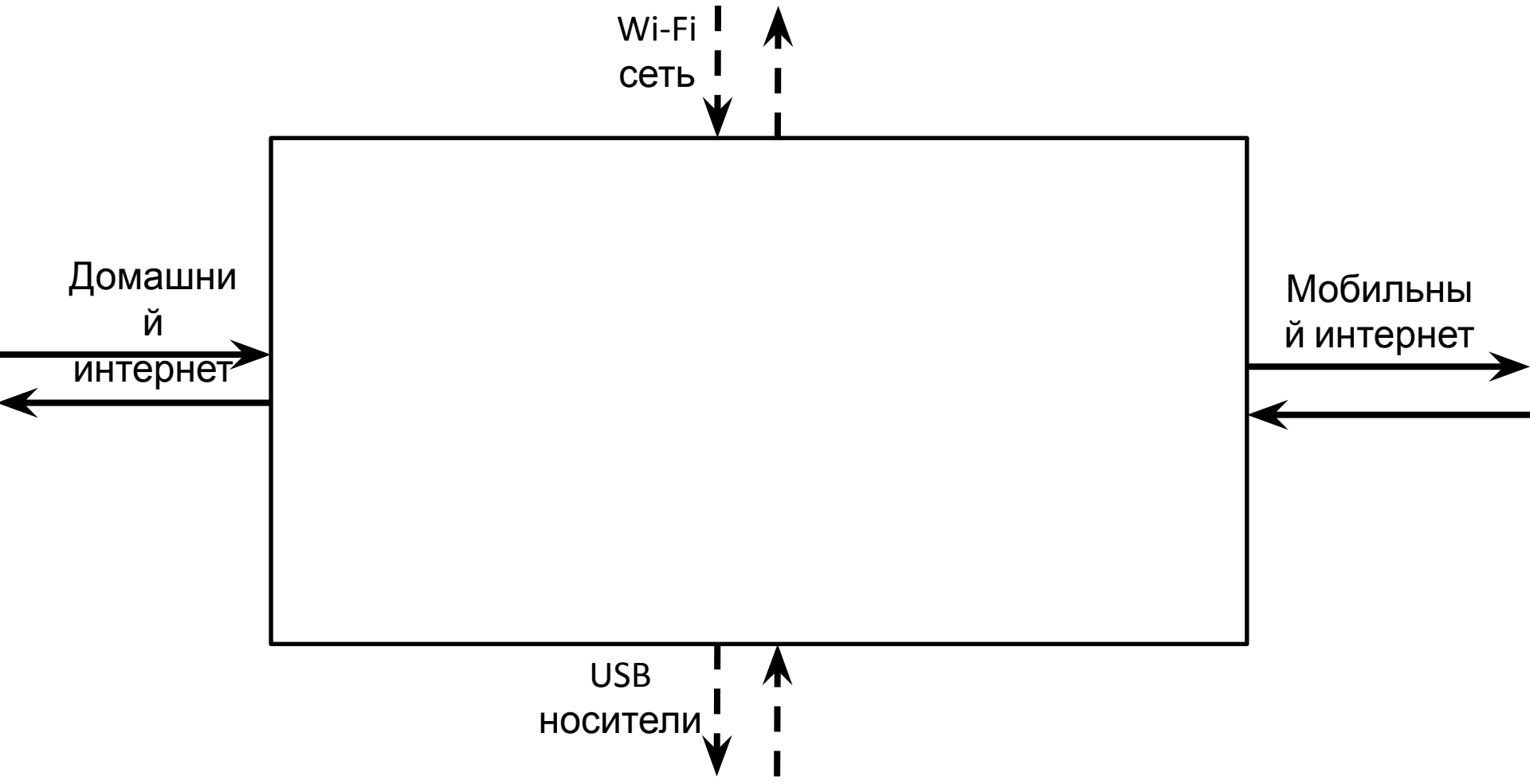
Потенциальная уязвимость границ – подключение сторонних устройств к домашней сети.

Открытость
(Сильно выражено)

Моя домашняя сеть способна подключаться к более крупным сетям посредством различных портов, являющихся одновременно входами и выходами. Используются 4 порта: домашний провайдер, подключаемый через роутер, мобильный оператор, подключаемый через сотовые вышки, подключение телефонов через общественные Wi-Fi сети и передача данных на компьютеры посредством флеш-носителей.

Потенциальная уязвимость портов – это недостаток информации о потенциально возможных Wi-Fi подключениях и возможность несанкционированного использования USB-портов.

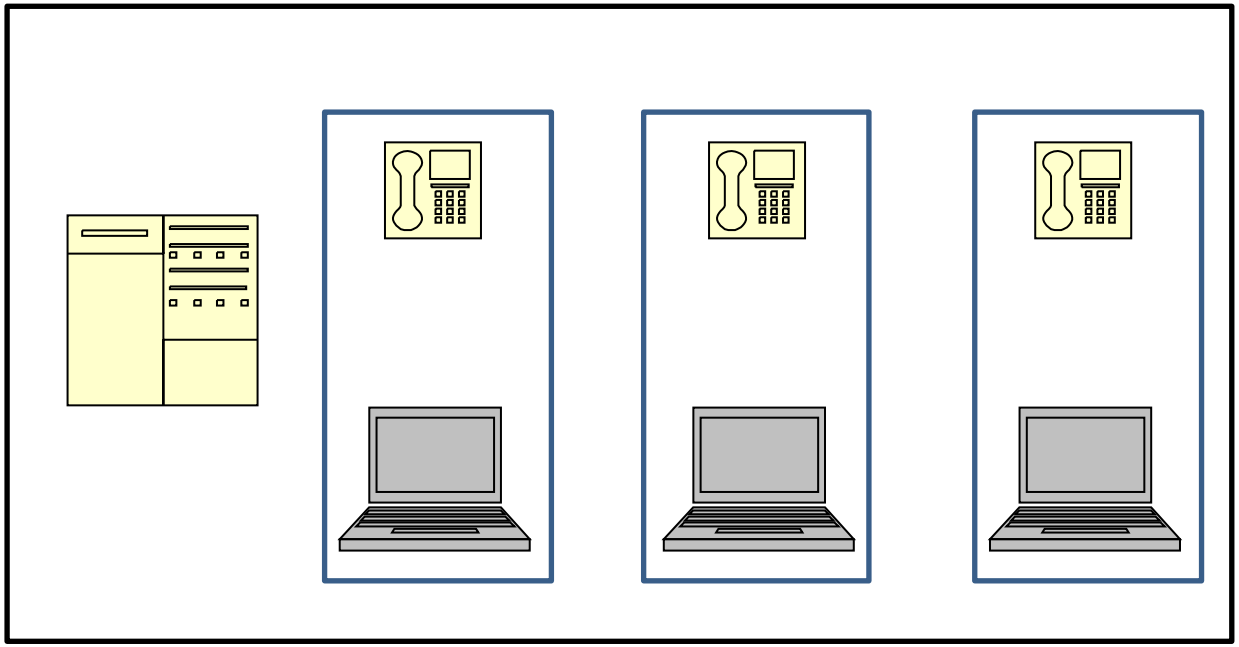
Модель «чёрный ящик»



Внутренняя неоднородность (Сильно выражено)

В моей домашней сети несколько элементов, разделяемых на 2 группы: компьютеры и телефоны. При этом их можно объединить в подсистемы, каждая из которых состоит из компьютера и телефона одного владельца. Кроме них, в сети ещё есть роутер, осуществляющий основную связь с внешним миром.

Структурная модель

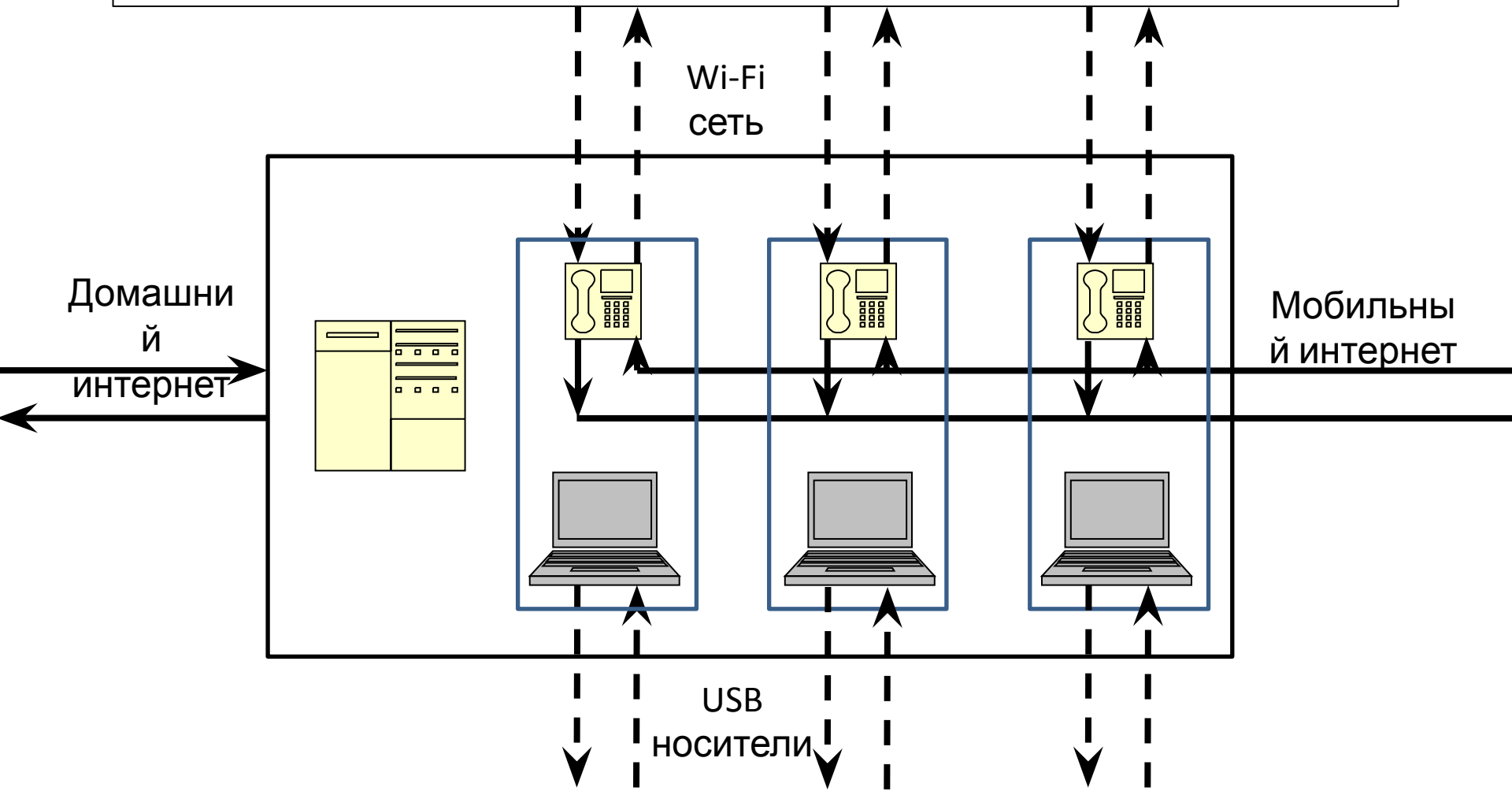


Структурированность (Сильно выражено)

Компьютеры и телефоны одного владельца могут соединяются вместе для обмена документами и изображениями. Обмен осуществляется посредством USB-кабелей. Но главное, что все домашние устройства подключены к роутеру, и осуществляют выход в Интернет через него.

Потенциальная уязвимость структуры – любая атака направленная на роутер отразится на всех других устройствах.

Модель связей



Функциональность (Сильно выражено)

В процессе работы система выдаёт большое количество информации, главным образом посредством экранов. Также информация может передаваться домашней сетью в Интернет через маршрутизатор по протоколу IPv4, посредством мобильной связи или через Wi-Fi сети, которые анализировать на порядок сложнее.

Стимулированность (Сильно выражено)

В процессе работы система получает большое количество информации, главным образом посредством клавиатуры и мыши для компьютера или сенсорного экрана для телефона. Также информация может передаваться домашней сетью в Интернет через маршрутизатор по протоколу IPv4, посредством мобильной связи или через Wi-Fi сети, которые анализировать на порядок сложнее.

Изменчивость
(Средне выражено)

Изменения в домашней сети редки, физические устройства меняются по мере необходимости, срок службы 5 - 10 лет. При этом программное обеспечение обновляется регулярно, при первой возможности.

Потенциальная уязвимость изменчивости – срок приспособления к сделанным изменениям.

Существование в изменяющейся среде (Слабо выражено)

Моя домашняя сеть существует в постоянно изменяющейся среде. Поэтому приходится приспосабливаться к этим изменениям, постоянно обновлять программное обеспечение, иногда аппаратное.

Потенциальная уязвимость – несвоевременное реагирование на произошедшие изменения.

Эмерджентность
(Слабо выражено)

Устройства домашней сети (кроме роутера) используются независимо друг от друга, при исключении любого из них все остальные продолжат нормально функционировать.

Неделимость на части (Сильно выражено)

Устройства домашней сети (кроме роутера) используются независимо друг от друга, но исключение любого из них из системы лишает её многих возможностей к достижению её целей.

Потенциальная уязвимость – исключение роутера из системы полностью остановит её функционирование в сети Интернет.

Ингерентность
(Сильно выражено)

Несмотря на то, что сама по себе домашняя сеть меняется нечасто, большинство изменений происходят в ответ на внешние воздействия, а не по хотению участников-людей. В основном поддерживается ПО, своевременно получающее обновления.

Потенциальная уязвимость – система меняется только при участии человека, он и является слабым звеном.

Целесообразность (Сильно выражено)

У моей домашней сети существует множество целей, при этом каждый из участников имеет свои приоритеты. Основные 3 цели: это обмен информацией, развлечение (компьютерные игры) и осуществление рабочих проектов.

Потенциальная уязвимость – наиболее рискованной с точки зрения безопасности является осуществление рабочих проектов, так как оно требует привлечения малознакомых источников и сторонних устройств.