Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)

Международная научная школа: «Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах»

Лекция: «Модели и методы параллельной обработки больших массивов данных при сборе и предварительной обработке информации для мониторинга и управления безопасностью в сетях Интернета вещей»

Саенко Игорь Борисович, д.т.н., профессор,
ведущий научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН

Учебные вопросы

1. **Проблема сбора и предварительной обработки информации для мониторинга и управления безопасностью в сетях Интернета вещей**
2. **Модели и методы параллельной потоковой обработки данных для мониторинга и управления безопасностью в сетях Интернета вещей**

Литература

Безопасность Интернета вещей

- Perera C. et al. **Context Aware Computing for The Internet of Things: A Survey** // IEEE Communications Surveys & Tutorials. – 2013. – P. 1–41.
- Roman R. et al. **Security in the Distributed Internet of Things** // Proc. of the 4th International Conference, INTRUST 2012. – 2012. – LNCS, vol. 7711. – P. 65–66.
- Babar S. et al. **Proposed security model and threat taxonomy for the internet of things (IoT)** // Proc. of the 3d International Conference on Network Security and Applications (CNSA 2010). – 2010. – CCIS, vol. 89. – P. 420–429.
- Suo H. et al. **Security in the Internet of Things: A Review** // Proc. of the 2012 International Conference on Computer Science and Electronics Engineering. Guangzhou, China. – 2012. – P. 648–651.
- Mayer Ch.P. **Security and Privacy Challenges in the Internet of Things** // Proc. of the WowKiVS 2009 (Workshops der Wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen 2009). Electronic Communications of the EASST. – 2009. – Vol. 17. – P. 1–12.

Потоковая обработка данных

- Gulisano, V. et al. **StreamCloud: A Large Scale Data Streaming System** // Proc. o f the 2010 International Conference on Distributed Computing Systems, p.126-137.
- Gulisano, V. et al. **StreamCloud: An Elastic and Scalable Data Streaming System** // IEEE Trans.on Parallel and Distributed Systems, Vol. 23, No. 12, December 2012, p. 2351-2365.

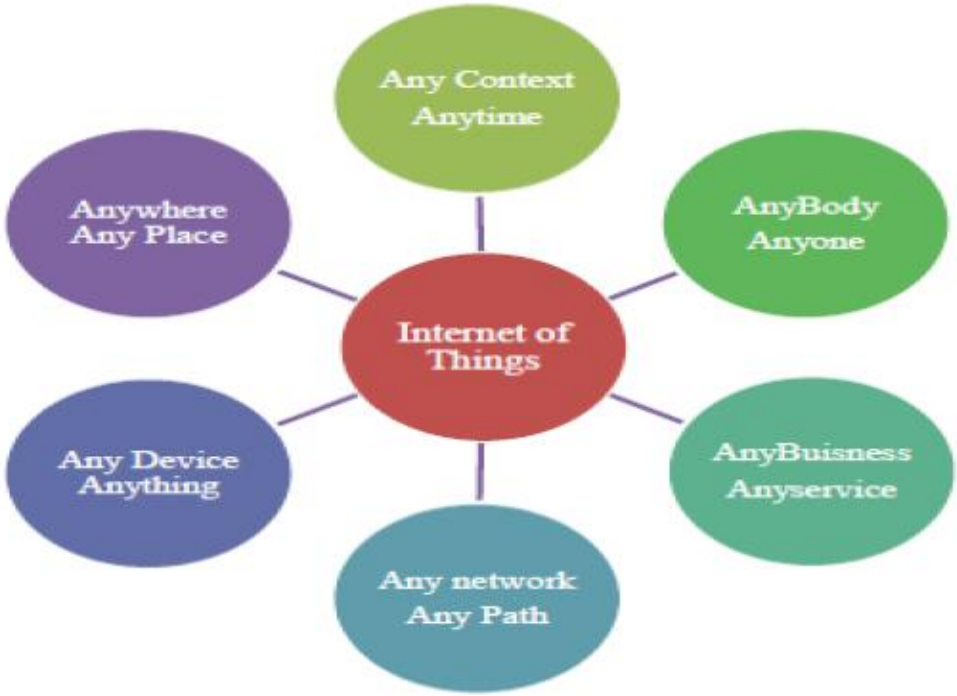
Учебный вопрос № 1

1. Проблема сбора и предварительной обработки информации для мониторинга и управления безопасностью в сетях Интернета вещей

- Понятие Интернета вещей
- Особенности угроз безопасности в Интернете вещей
- Особенности мониторинга и управления безопасностью в Интернете вещей

Понятие Интернета вещей

Распределенные сети электронных потребительских устройств, или «Интернет вещей» - новое поколение сетевых компьютерных инфраструктур, которые существенно расширяют возможности создания и области применения распределенных автоматизированных систем различного назначения в современном информационном обществе.



Принципы построения:

а) в любое время предоставление любого контекста (Any Context Anytime);
б) любой пользователь может иметь любые права (AnyBody Anyone);
в) любой бизнес-процесс поддерживается сервисами сети (AnyBuisiness Anyservice);
г) любой путь в любой сети (Any Path Any network);
д) любое устройство как любая вещь (Any Device Anything);
е) в любом месте доступ (Any Place Anywhere).

Архитектура типовой сети Интернета вещей

Характеристика уровней архитектуры Интернета вещей

Уровень	Количество в 2020 году	Элементы	Характеристики
1.Восприятия	Нет оценки	Штрихкод, RFID	Элементы содержат данные, которые могут быть использованы другими элементами автоматически. Элементы имеют уникальный идентификатор.
2.Сетевой	1 триллион	Сенсор, контроллер	Элементы имеют каналы и методы для взаимодействия с другими элементами. Элементы имеют каналы и методы для взаимодействия со своей средой.
3.Прикладной	50 млрд.	Рабочая станция, ноутбук, смартфон	Элементы имеют каналы и методы для взаимодействия с пользователями.

Области применения Интернета вещей

Наиболее популярные области применения сетей Интернет вещей:

а) медицинские информационные инфраструктуры;

б) транспортные инфраструктуры;

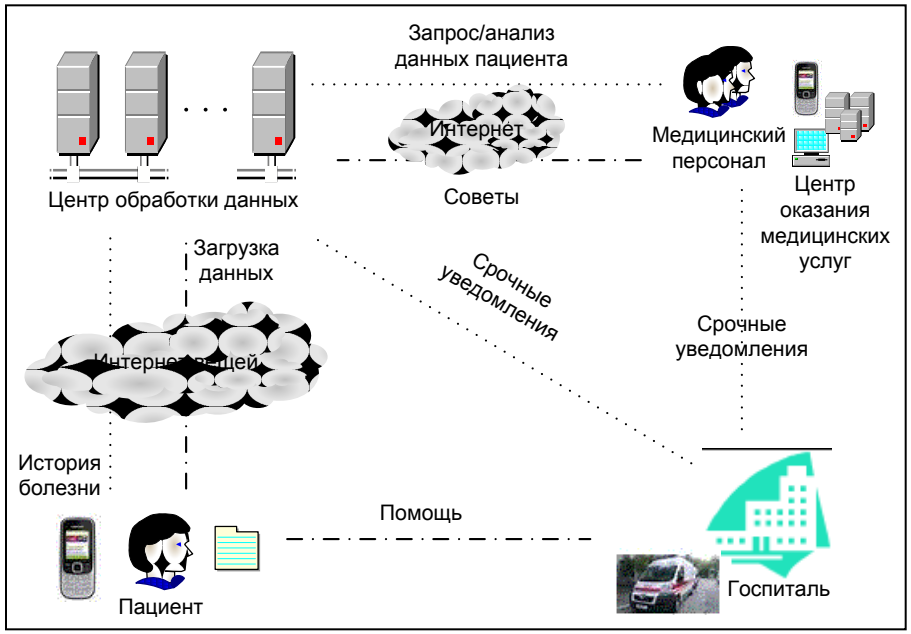
в) системы мониторинга охраняемой территории

г) интеллектуальные системы управления домом;

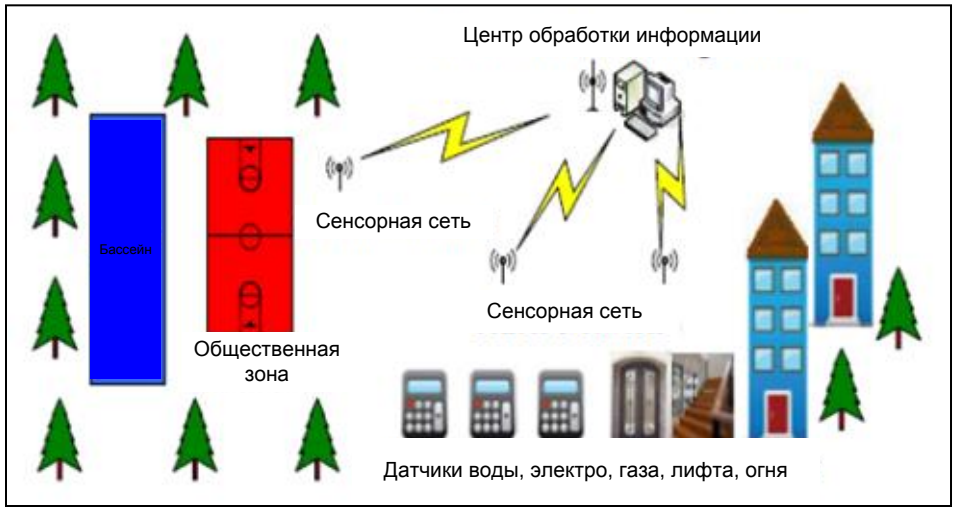
д) сети потребления электроэнергии, оснащенные интеллектуальные счетчиками;

е) системы промышленного производства и т.д.

Примеры:



Система удаленного мониторинга состояния здоровья



Система обеспечения безопасности в общественных местах

Требования по безопасности Интернета вещей

Высокоуровневые требования по безопасности IoT:

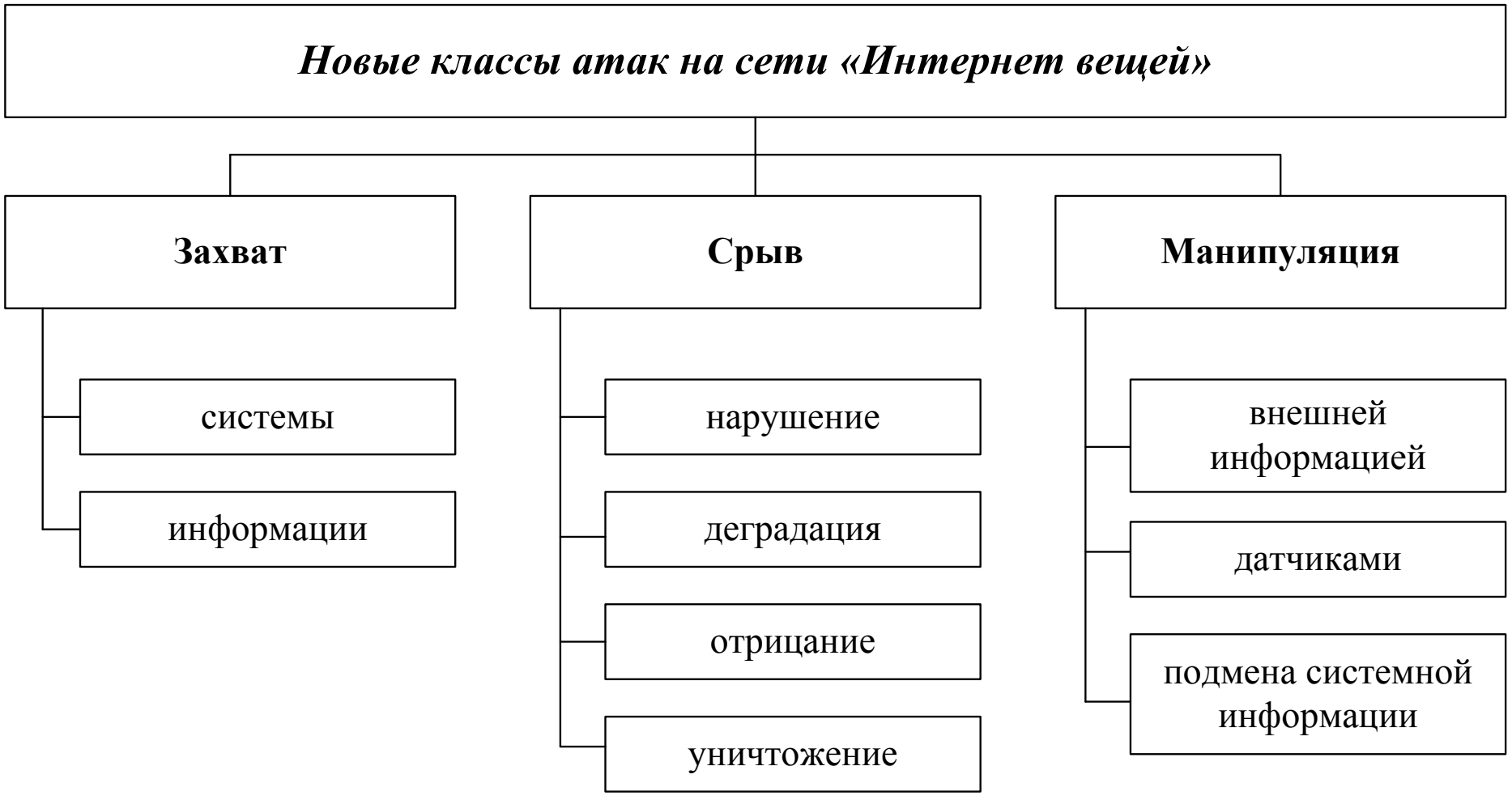
- Идентификация пользователей
- Безопасность хранения
- Управление идентификацией
- Безопасность каналов связи
- Доступность
- Безопасность сетевого доступа
- Безопасность содержания
- Безопасность приложений
- Защита от взлома

№ п/п	Наименование требования	Характеристика требования
1	Устойчивость к атакам	Система должна избегать единичных отказов и должна адаптироваться к отказам узлов сети, возникающих вследствие воздействия атак различного рода
2	Аутентификация данных	Данные, касающиеся адресной информации и характеристик объекта, должны быть аутентифицированы
3	Контроль доступа	Поставщики информации должны быть в состоянии осуществлять контроль доступа к поставляемым данным
4	Приватность пользователя	Только поставщик информации может иметь возможность идентифицировать на основе наблюдений информацию, связанную с конкретным потребителем; по крайней мере, сделать это другим лицам должно быть крайне затруднительно

Угрозы безопасности Интернета вещей

№ п/п	Типы угроз	Примеры угроз
1	Коммуникационные угрозы	- Отказ в обслуживании - Подмена (спуфинг) - Вставка (инъекция)
2	Угрозы управлению идентификацией	- Угрозы аутентификации - Угрозы авторизации - Угрозы приватности и контролю доступа
3	Физические угрозы	- **Микрозондирование** - **Обратный инжиниринг**
4	Угрозы безопасности встроенных компонентов	- Побочные каналы - **Манипуляция (подделка) данных** - Угрозы аутентификации устройств - Угрозы безопасной среде
5	Угрозы безопасности управления памятью	- Угрозы управлению ключами - Угрозы конфиденциальности - Угрозы целостности
6	Угрозы динамическому связыванию имен	- Угрозы механизмам именования и адресации - Угрозы интеграции сервисов и имен - Угрозы управлению псевдонимами

Новые классы атак в сетях Интернета вещей



Задачи мониторинга безопасности в IoT

Основные задачи, решаемые системой мониторинга и управления безопасностью:

а) **сбор, обработка и анализ** событий безопасности, поступающих в систему из множества гетерогенных источников;

б) **обнаружение** в реальном масштабе времени атак и нарушений критериев и политик безопасности;

в) оперативная **оценка** степени защищенности активов (информационных, телекоммуникационных и других ресурсов);

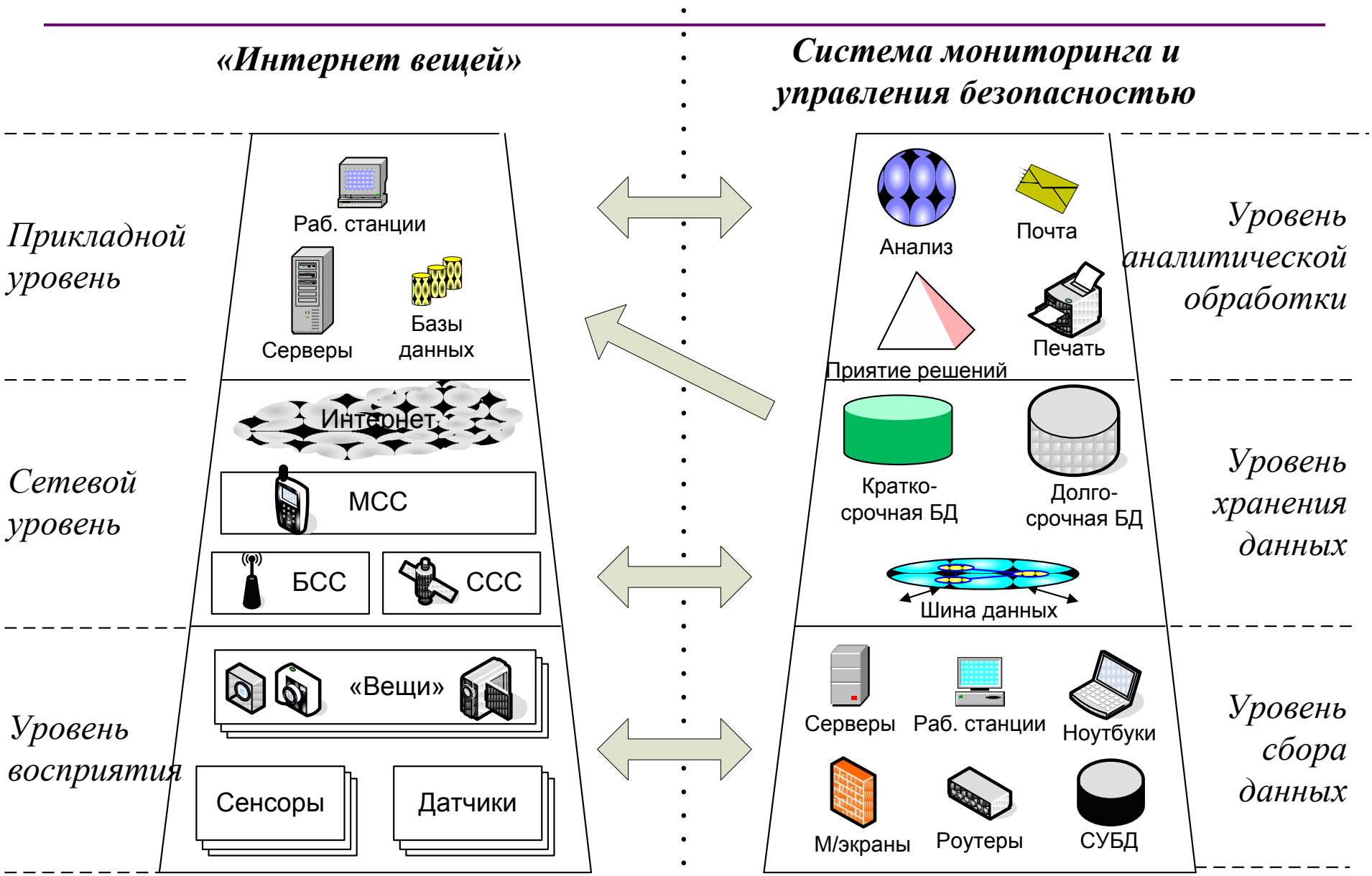
г) принятие эффективных **решений** по защите информации;

д) формирование отчетных **документов**.

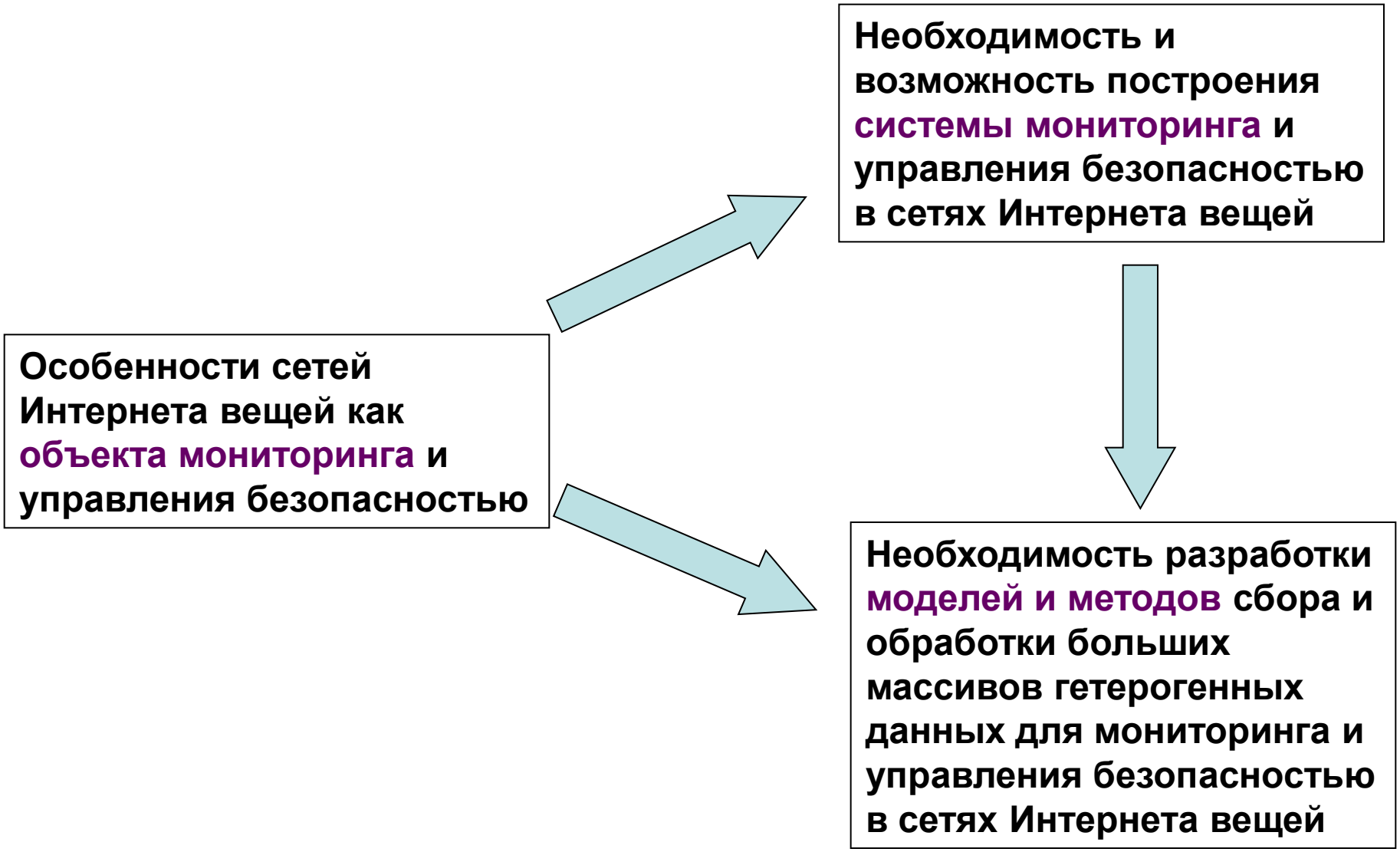
Источники данных для мониторинга:

1. серверы,
2. рабочие станции,
3. сетевые устройства,
4. программные комплексы.
5. физические сенсоры и датчики.

Сравнение архитектур SIEM и IoT



Проблема


Необходимость и возможность построения системы мониторинга и управления безопасностью в сетях Интернета вещей
Особенности сетей Интернета вещей как объекта мониторинга и управления безопасностью
Необходимость разработки моделей и методов сбора и обработки больших массивов гетерогенных данных для мониторинга и управления безопасностью в сетях Интернета вещей

Учебный вопрос № 2

2. Модели и методы параллельной потоковой обработки данных для мониторинга и управления безопасностью в сетях Интернета вещей

- Понятие «потоковой обработки данных»
- Основные операторы потоковой обработки данных
- Схемы и стратегии параллельной потоковой обработки данных

Понятие CEP

CEP (Complex Event Processing) – технология оперативной (онлайн) обработки однородных данных, поступающих на узел обработки в виде потока.

Основные свойства CEP:

- **Поток *S*** – это бесконечная последовательность событий
- **Событие** – это кортеж, имеющий предопределенную **схему** $(A_1, A_2, ..., A_n)$
- **Схема потока** равна схеме события

Основные операторы CEP

«Без сохранения состояния»:

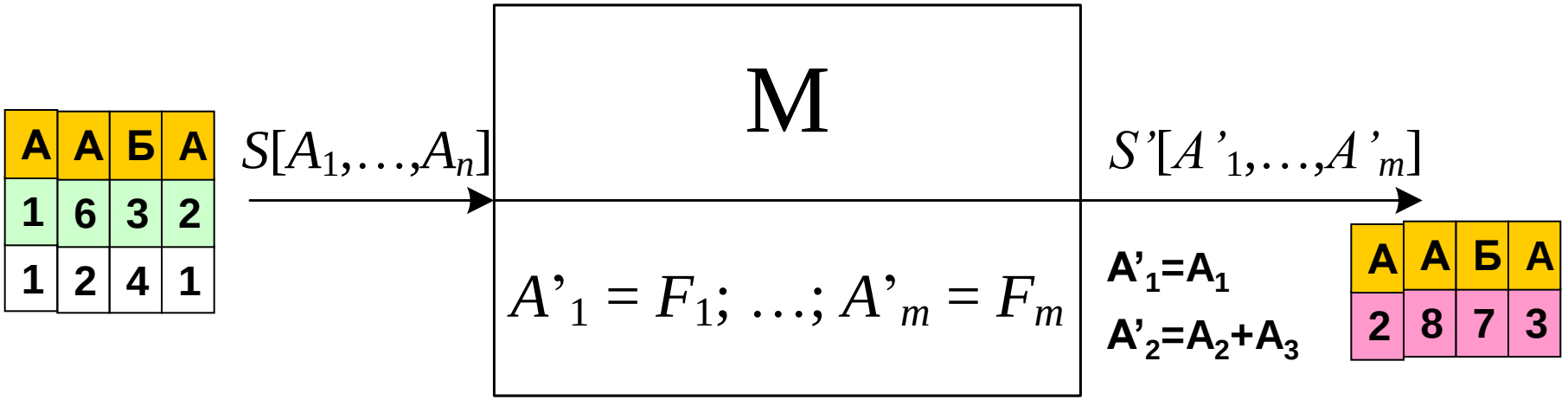
- оператор *Map* («отражение»);
- оператор *Filter* («фильтрация»);
- оператор *Union* («соединение»).

«С сохранением состояния»:

- оператор *Aggregate* (агрегации);
- оператор *Join* (соединения).

Оператор *Map*

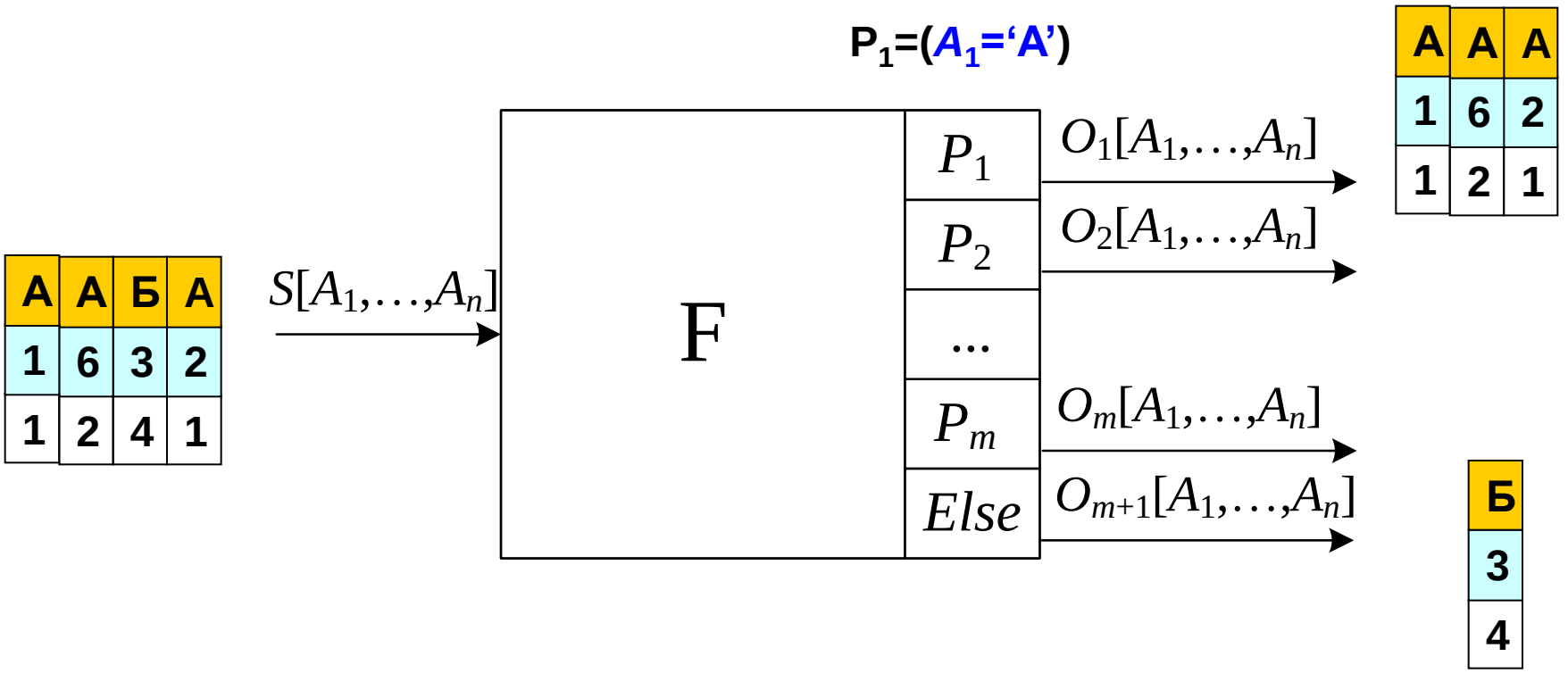
Оператор *Map* - обобщенный оператор проекции



S' = Map {A'1 = F1; …; A'm = Fm} (S)

Оператор *Filter*

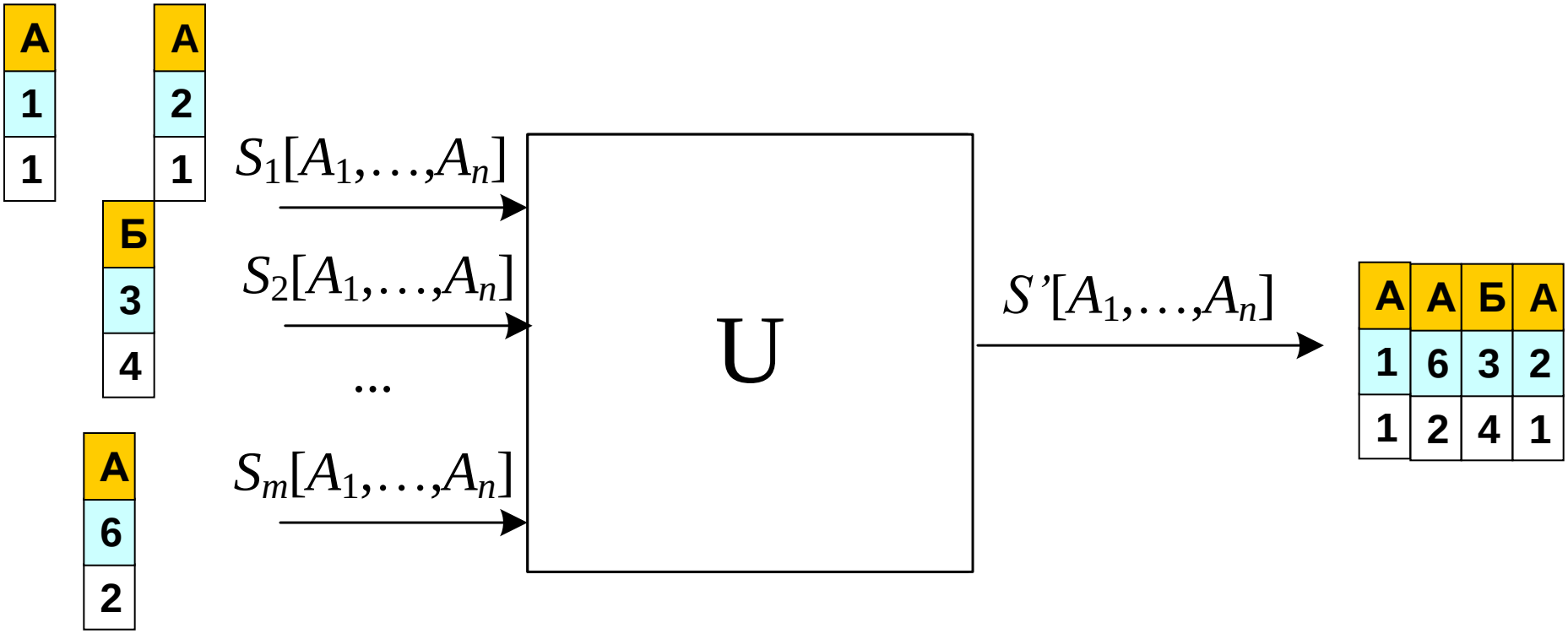
Оператор *Filter* - оператор выбора (селекции)



Filter **{(*P*$_1$; *O*$_1$); …; (*P*$_m$; *O*$_m$); *O*$_{m+1}$}** ***(S)***

Оператор *Union*

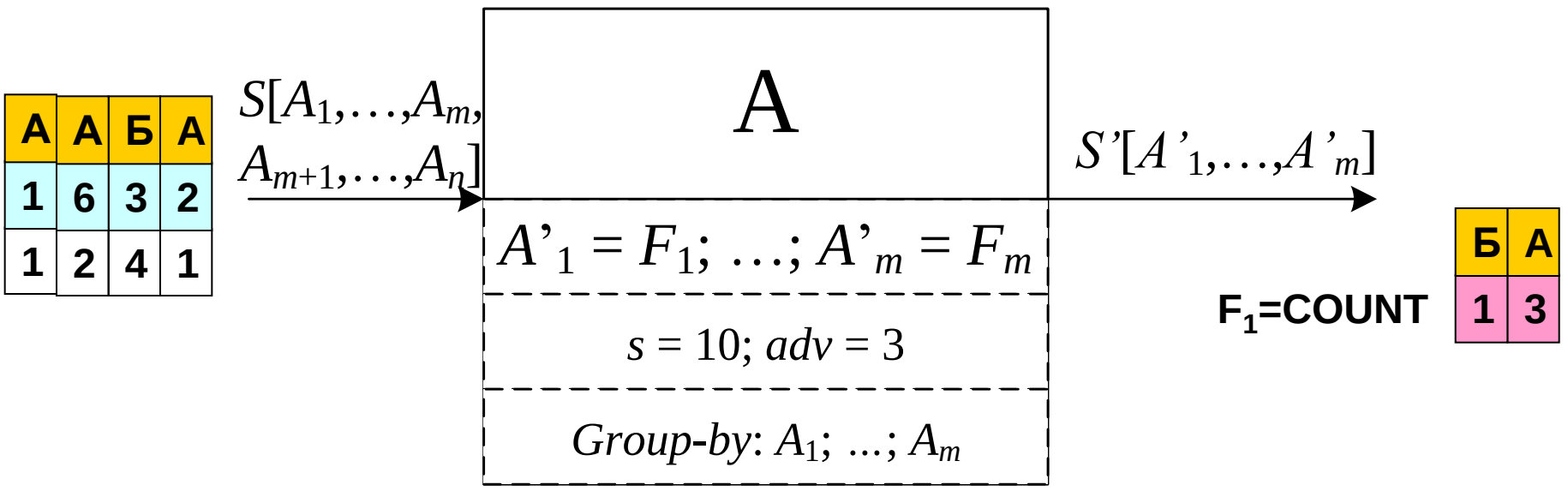
Оператор *Union* – объединение потоков



***Union* (S_1, …, S_m)**

Оператор *Aggregate*

Оператор *Aggregate* применяет некоторую функцию к двигающимся окнам записей входного потока вместе проекцией



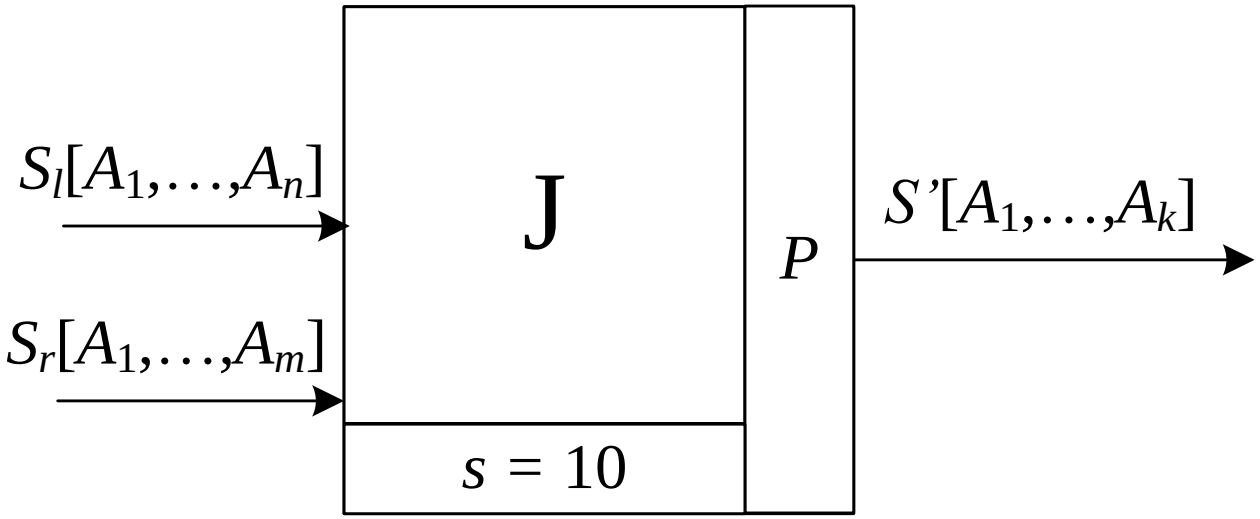
Aggregate **{*A'*$_1$ = *F*$_1$; …; *A'*$_m$ = *F*$_m$; *s*; *adv*; *Group-by* (*A*$_1$; …; *A*$_m$)}(*S*),**

Оператор *Join*

Оператор *Join* – оператор соединения

h	*f*	*g*
2	2	3

В	Б	А
3	3	2

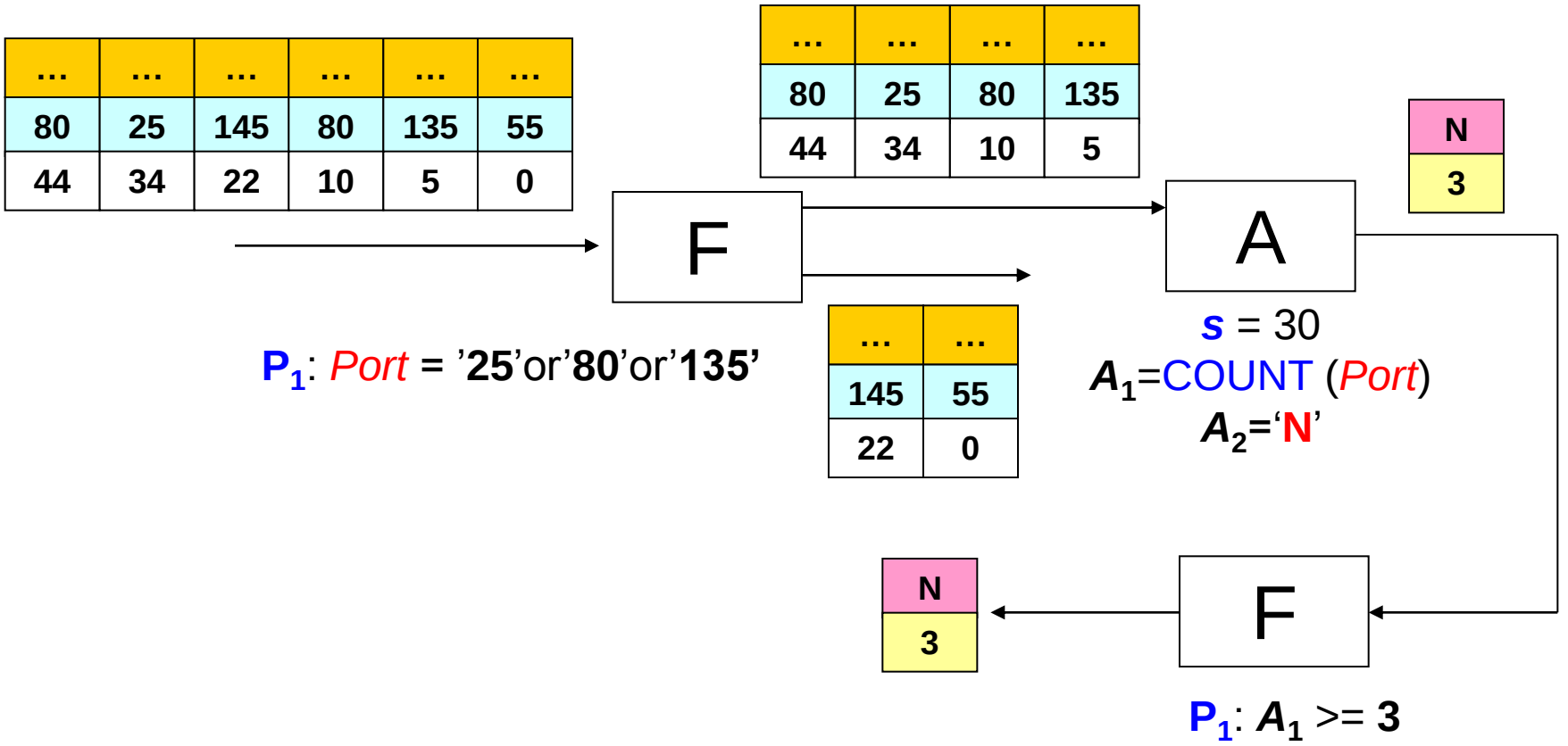


g	*g*	*h*	*f*
В	Б	А	А
3	3	2	2

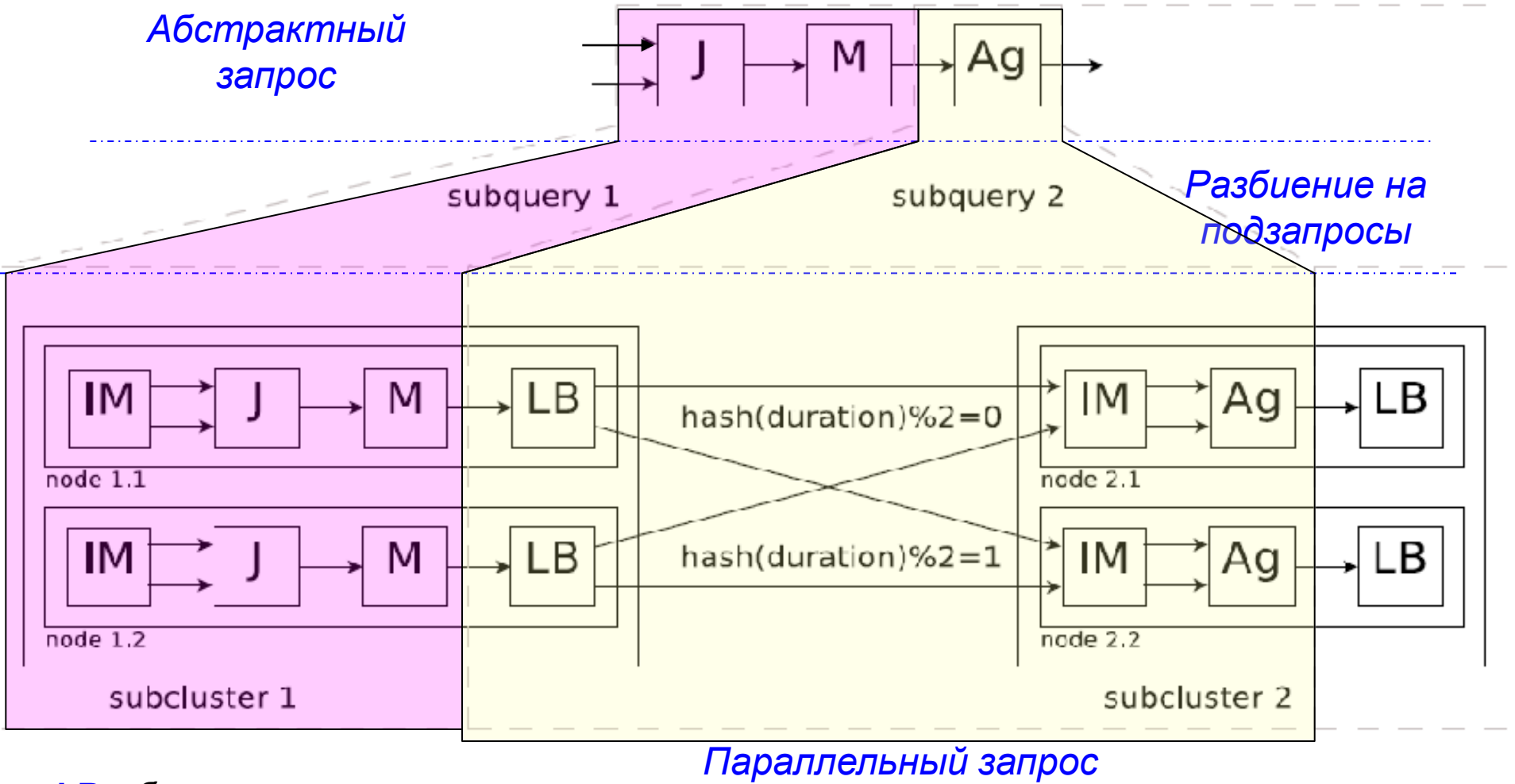
***Join* {*P*, *s*}(S_l, S_r)**

Пример применения *CEP*

ЗАПРОС: выдавать предупреждение каждый раз, когда в течение последних **30 секунд** в потоке будет обнаружено **3 обращения** к порту назначения, равняющемуся либо **25**, либо **80**, либо **135**.



Распараллеливание запроса

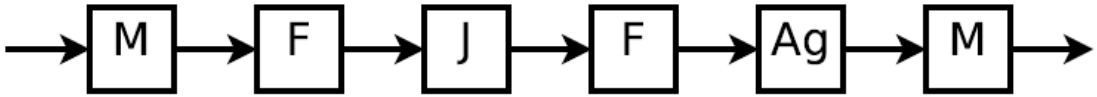


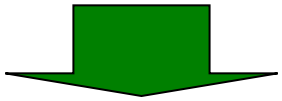
LB – балансировщик нагрузки

IM – смеситель входной

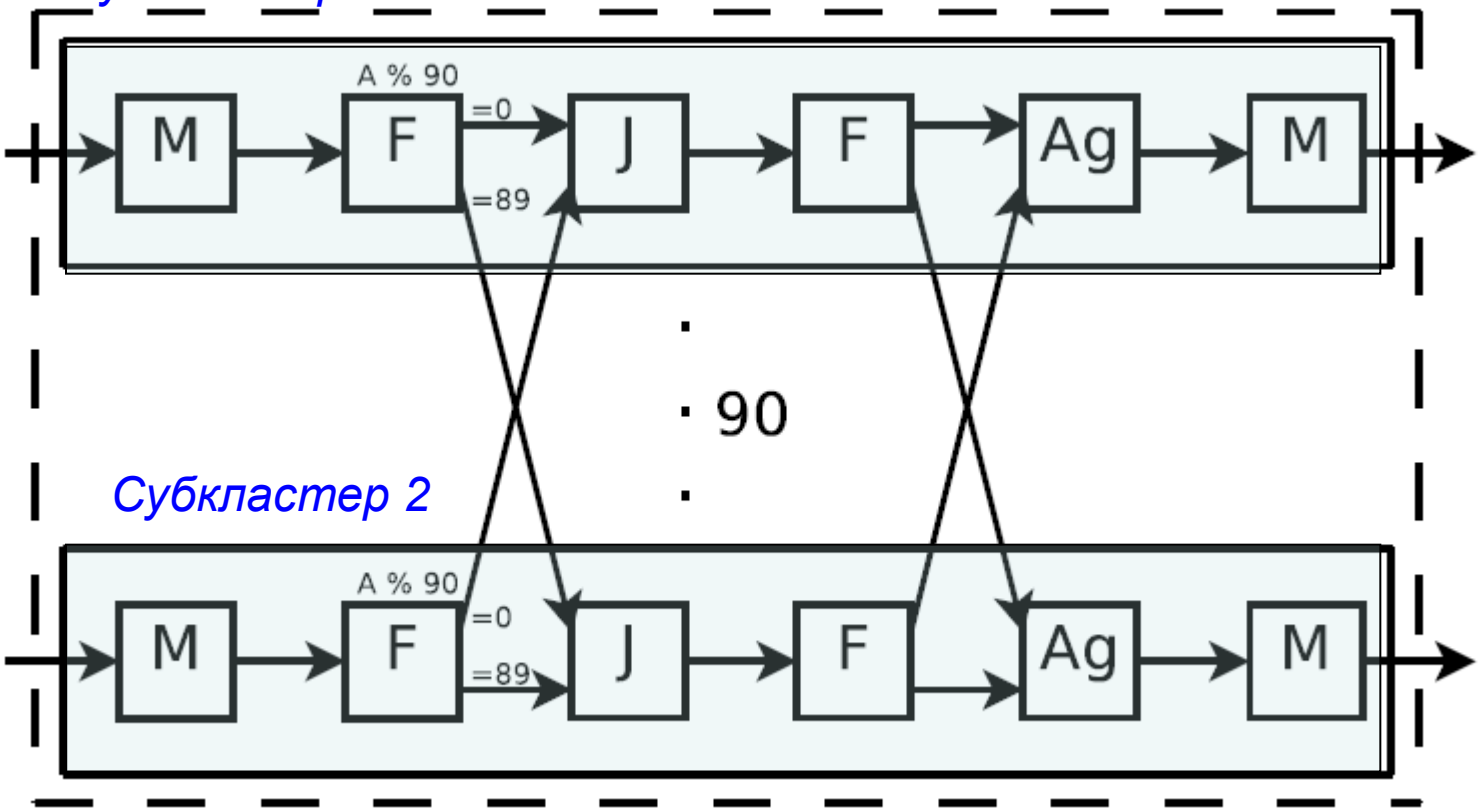
Стратегия «Запрос - кластер»

Абстрактный запрос



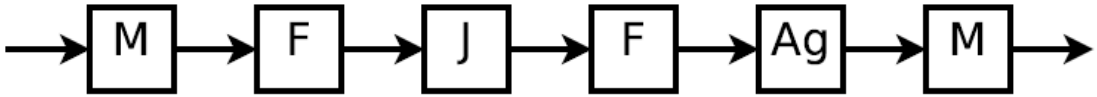


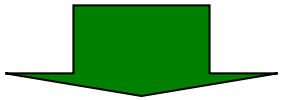
Субкластер 1



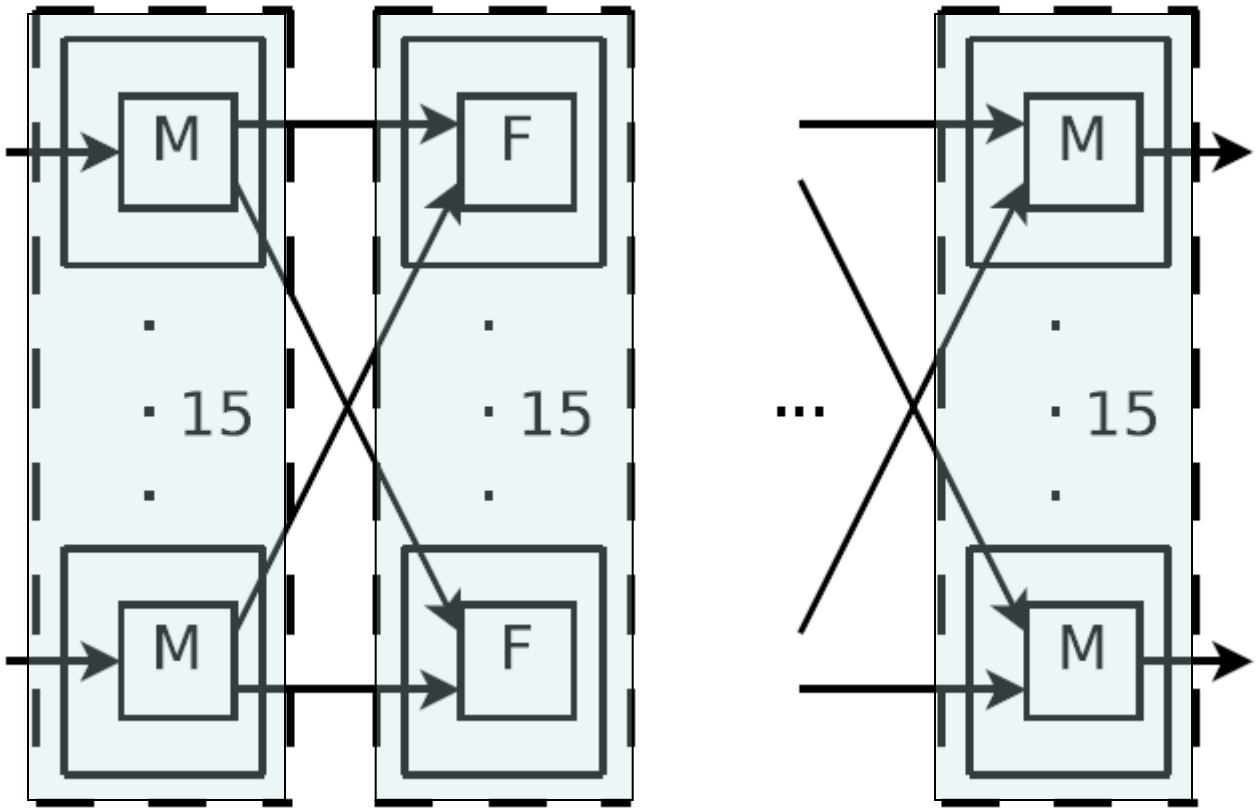
Стратегия «Оператор - кластер»

Абстрактный запрос

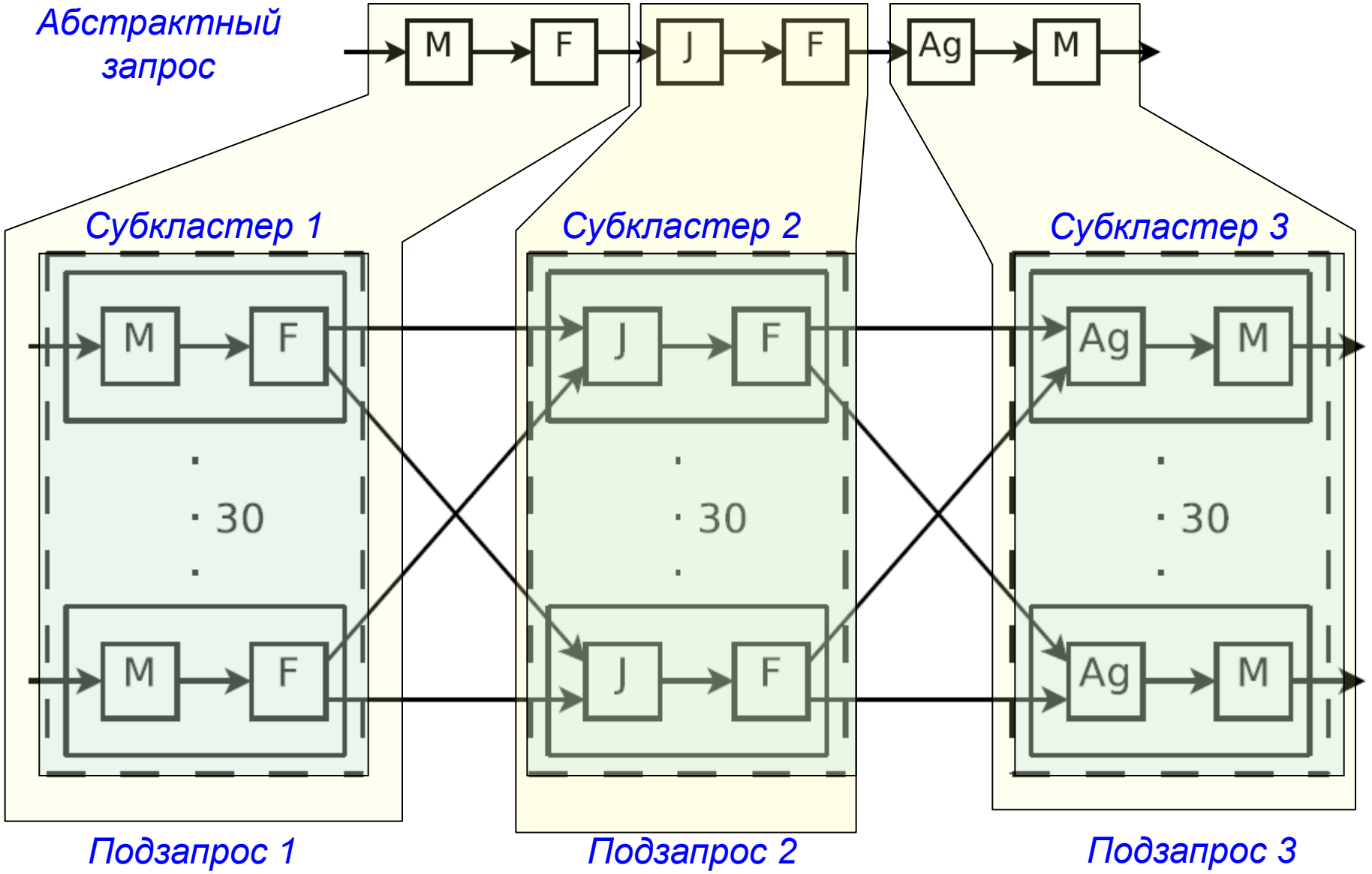




Субкластер 1 *Субкластер 2* *Субкластер 6*



Стратегия «Подзапрос - кластер»



Заключение

1. **Оперативная (онлайн) обработка** больших массивов гетерогенных данных для мониторинга и управления безопасностью в сетях Интернета вещей является **важной проблемой**.
2. Технология потоковой обработки данных **Complex Event Processing (CEP)** является одним их средств решения данной проблемы
3. **Распараллеливание** потоковой обработки запросов, необходимое для поддержания требуемой масштабируемости системы мониторинга и управления безопасностью в сети Интернета вещей, может осуществляться с применением различных **стратегий**.
4. Вопросы **анализа и реализации** стратегий распараллеливания обработки запросов на узлах Интернета вещей является **перспективным научным направлением**, требующим соответствующего исследования.