

УНИВЕРСИТЕТ ИТМО

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:  
MR. ROBOT В РЕАЛИЯХ РОССИЙСКОГО  
УНИВЕРСИТЕТА

ДОКЛАДЧИК:

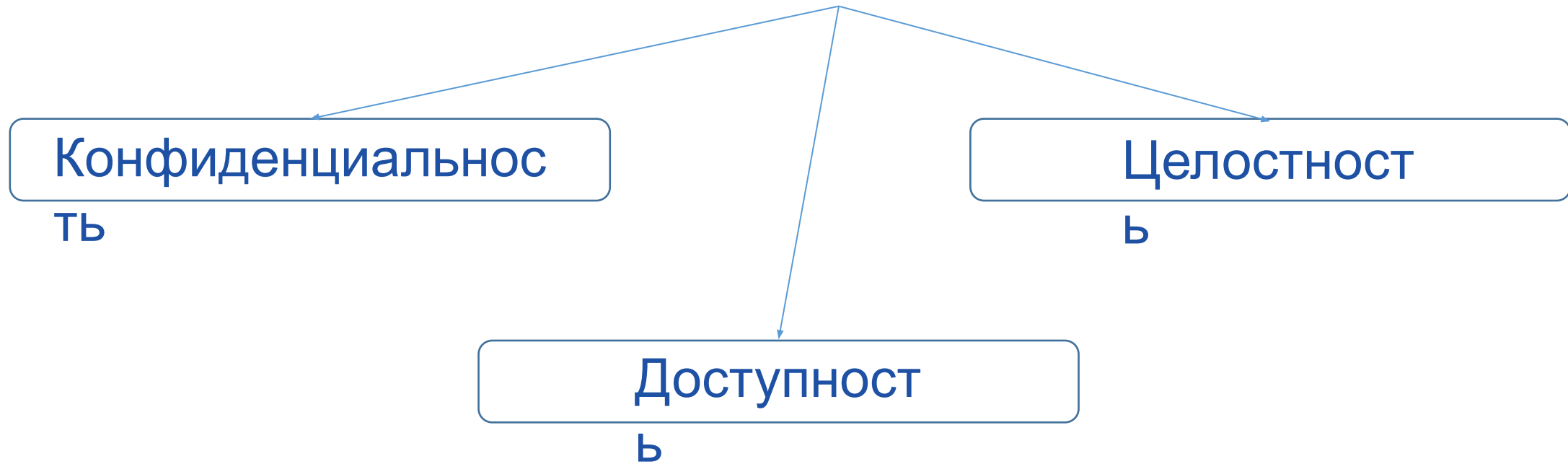
МАРИНЕНКОВ ЕГОР ДЕНИСОВИЧ

КОВАЛЕНКО АЛЕКСАНДР ВАЛЕРЬЕВИЧ

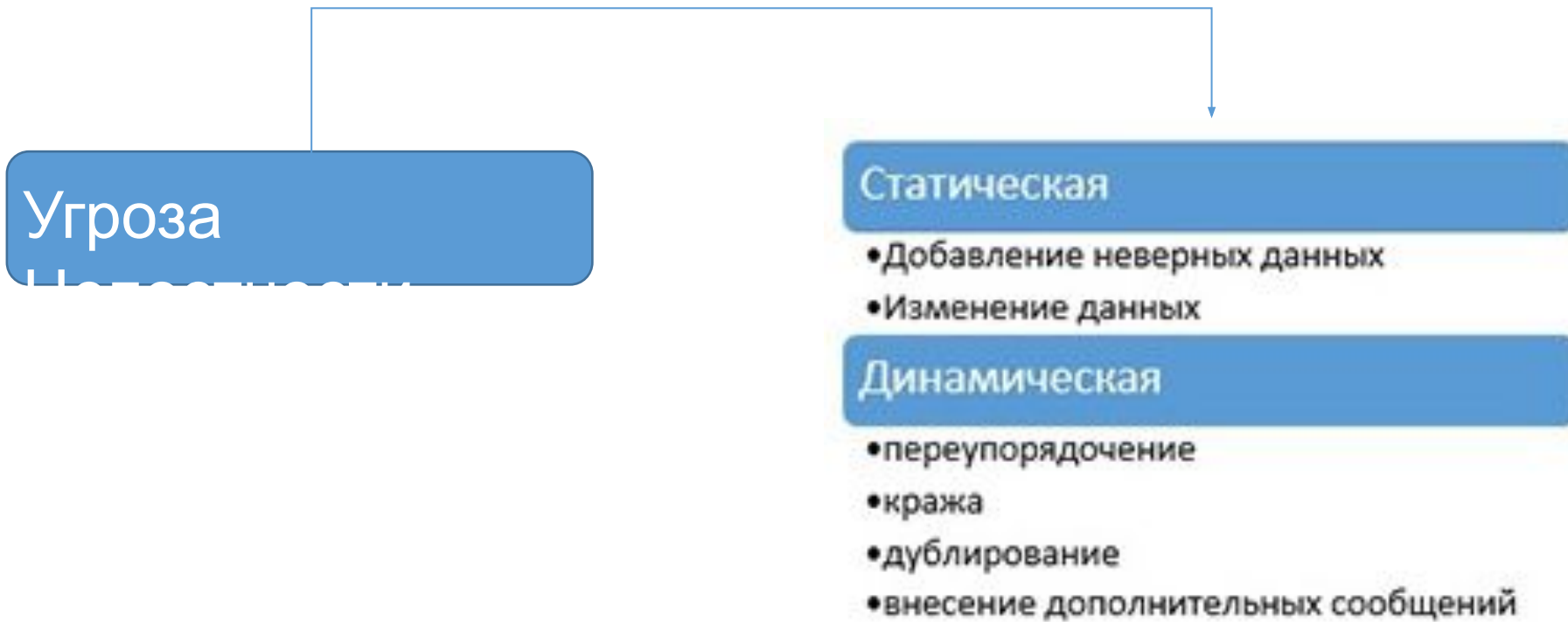
САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

САНКТ-ПЕТЕРБУРГ

# Информационная безопасность



# Классификация видов угроз ИБ



# Классификация видов угроз ИБ

## Угроза

### Внутренний отказ информационной системы

- нарушение от установленных правил эксплуатации
- выход системы из штатного режима эксплуатации
- ошибки при (пере)конфигурировании системы
- Вредоносное программное обеспечение
- отказы программного и аппаратного обеспечения
- разрушение данных
- разрушение или повреждение аппаратуры

### Отказ поддерживающей инфраструктуры

- нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
- разрушение или повреждение помещений
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности

# Классификация видов угроз ИБ

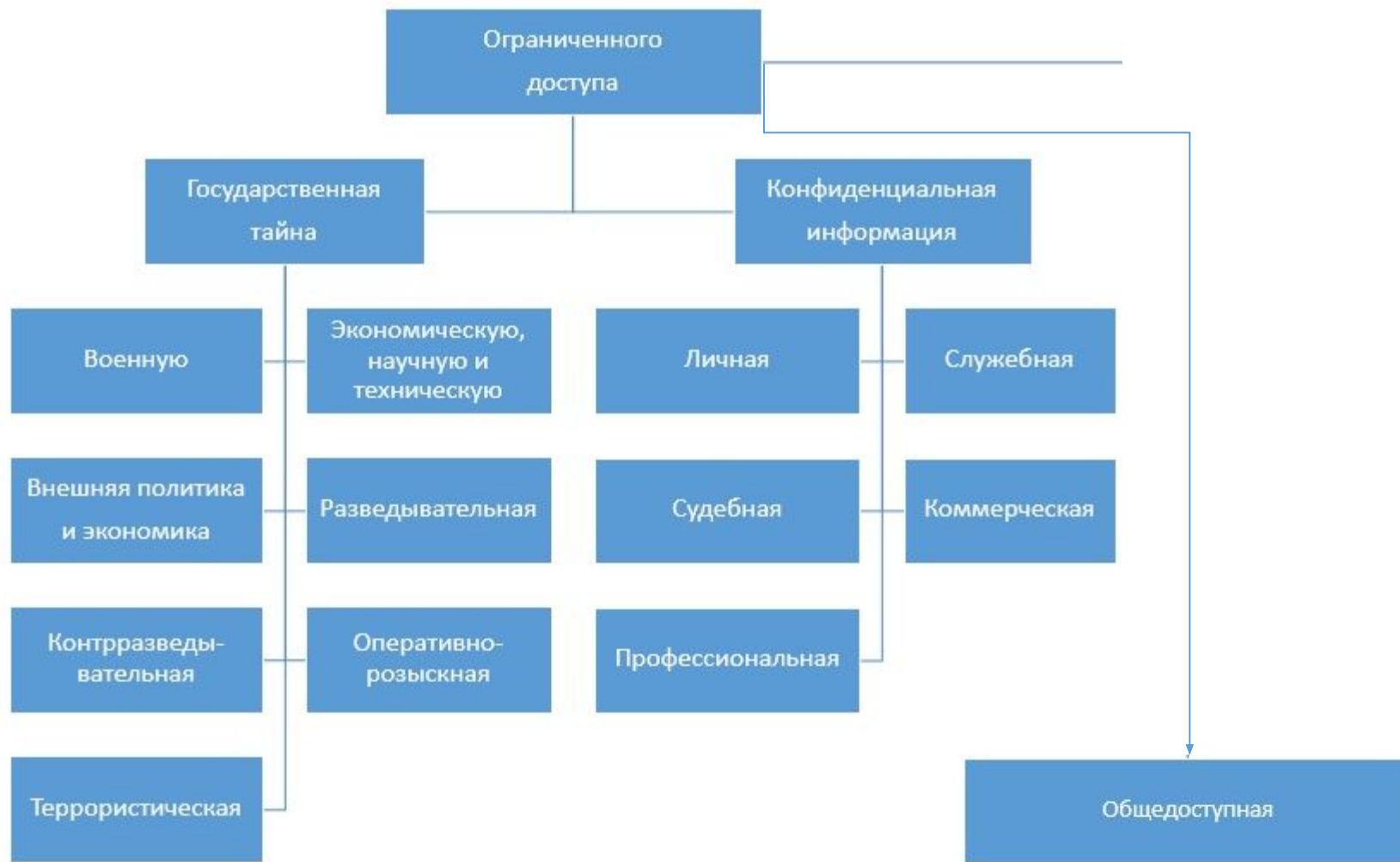
Угроза



Угрозы

- Служебной информации
- Предметной информации

# Виды



# Виды



## Модель информационной безопасности





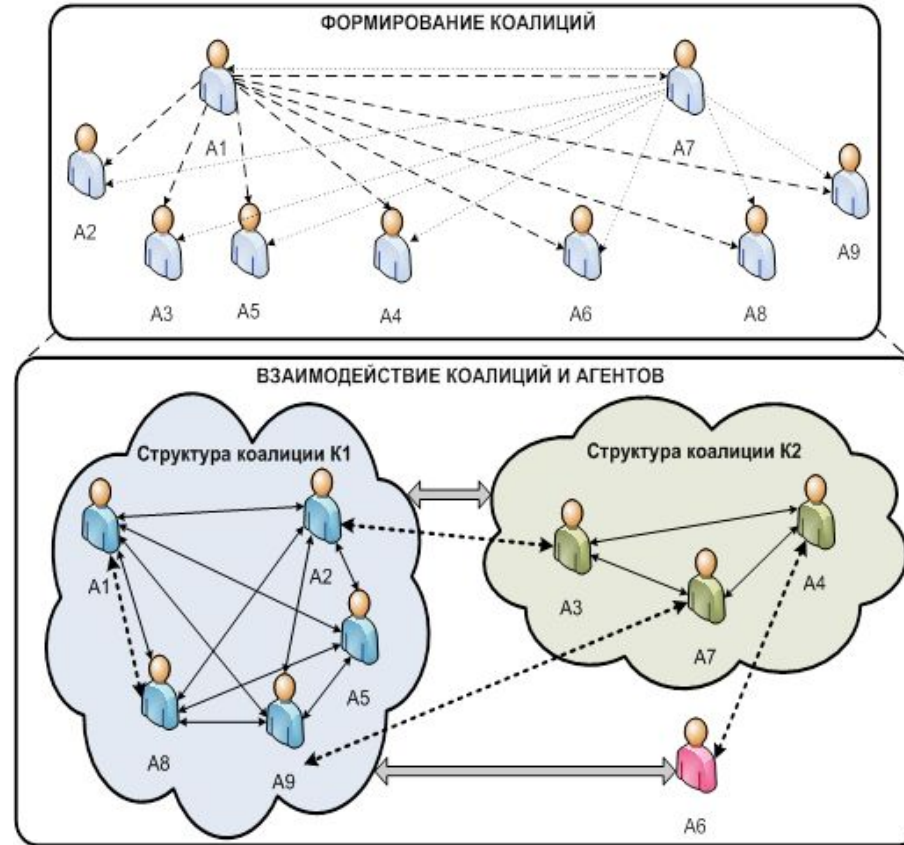
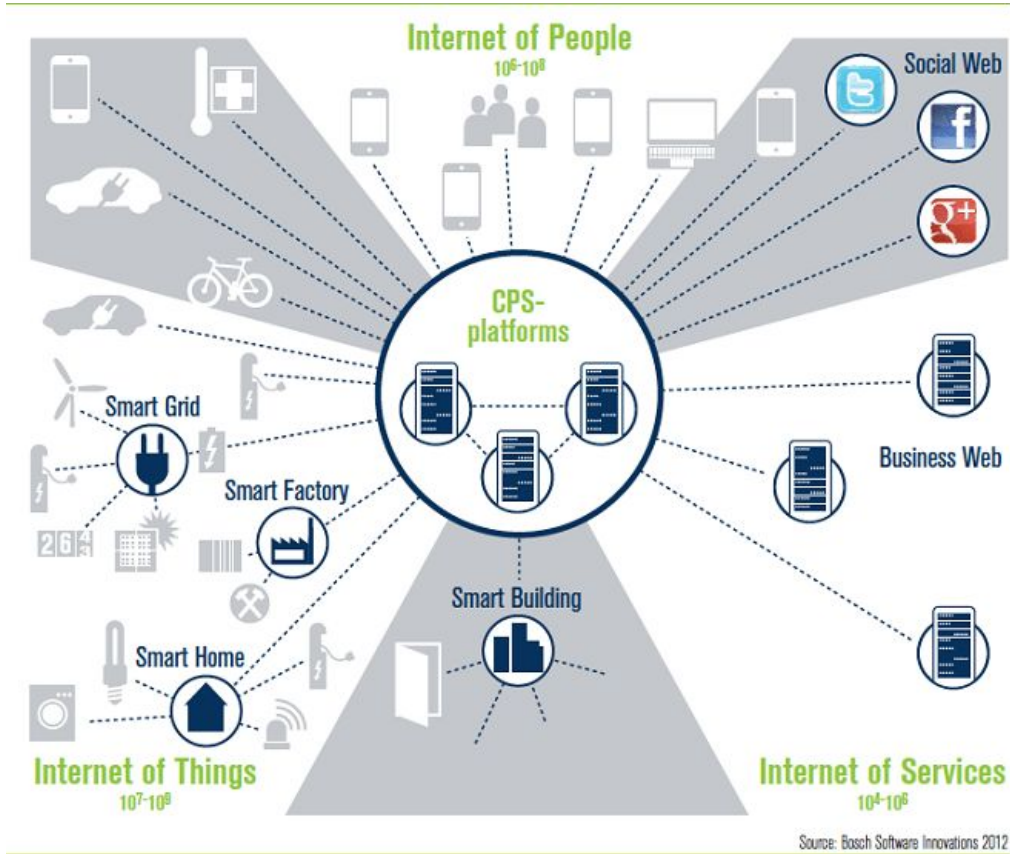
## Модель информационной безопасности



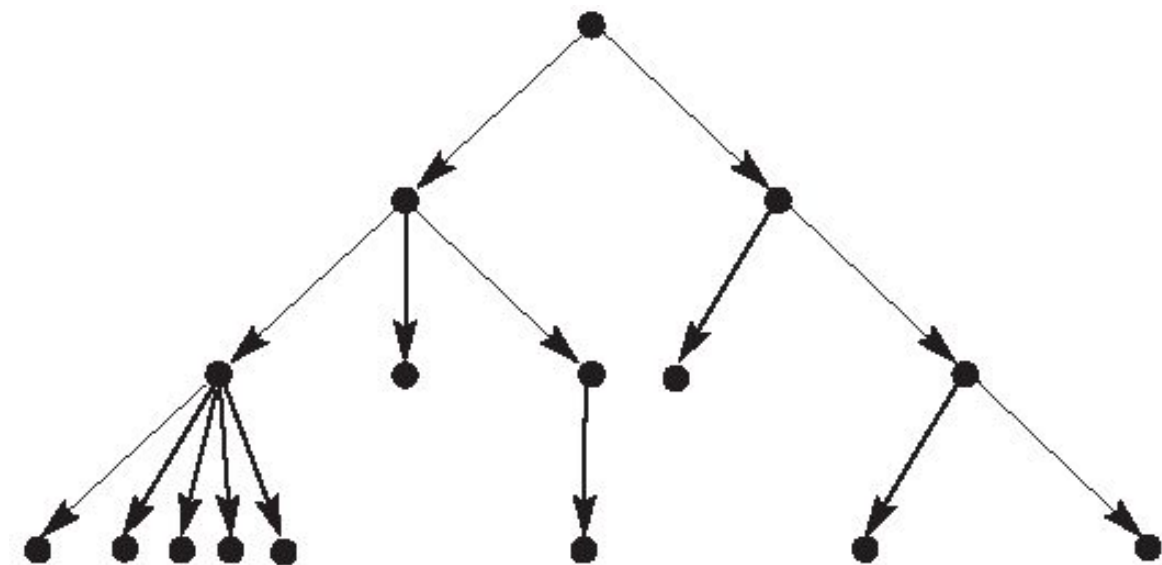
## Модель информационной безопасности



# МУЛЬТИАГЕНТНЫЕ СИСТЕМЫ

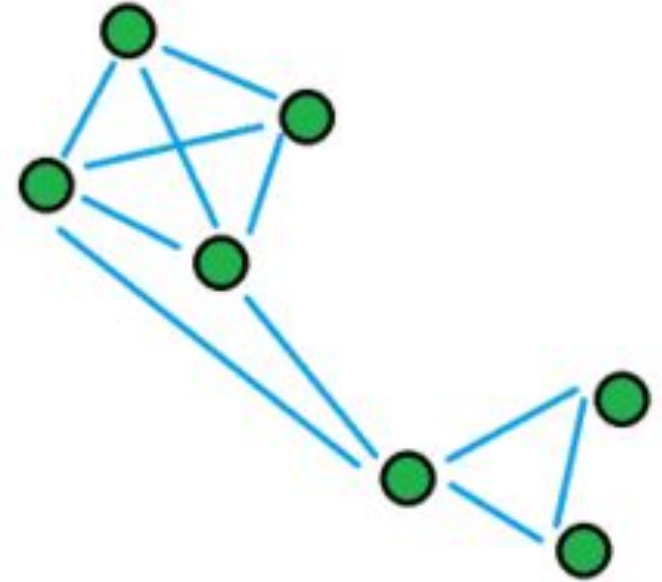


## АКТУАЛЬНОСТЬ

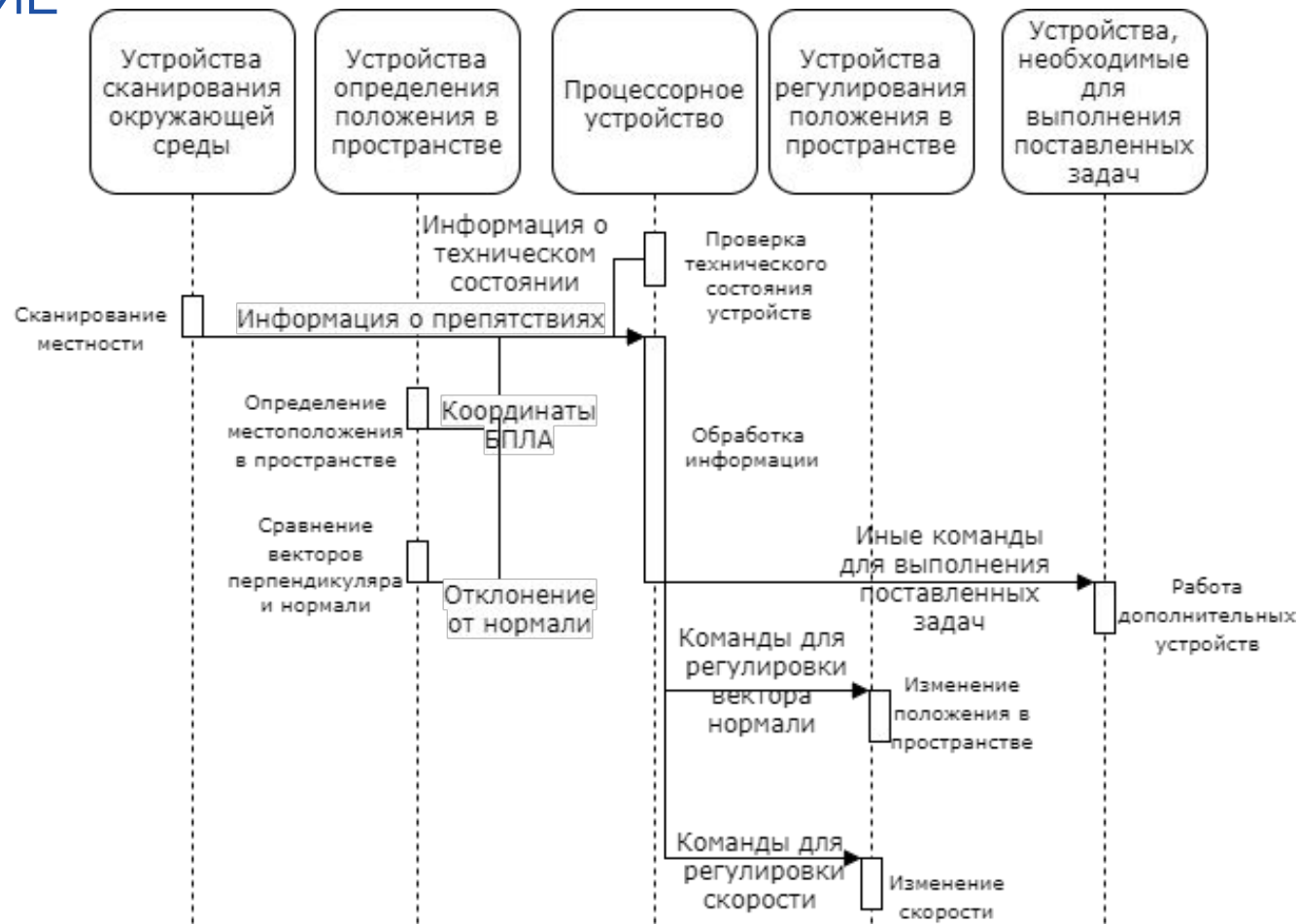


## САМООРГАНИЗУЮЩАЯСЯ СИСТЕМА

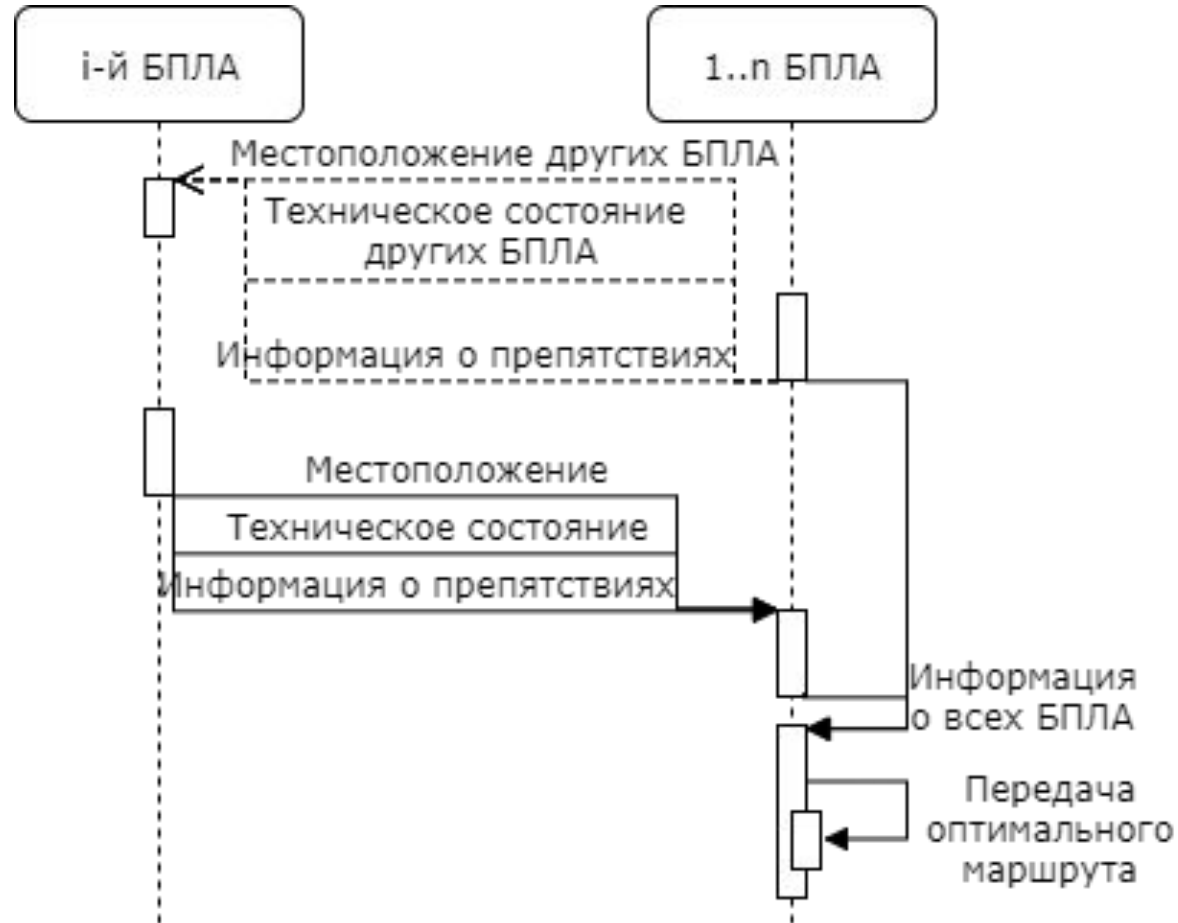
**Самоорганизующаяся система** – сложная динамическая система, способная при изменении внешних или внутренних условий ее функционирования и развития сохранять или совершенствовать свою организацию с учетом прошлого (накопленного) опыта.



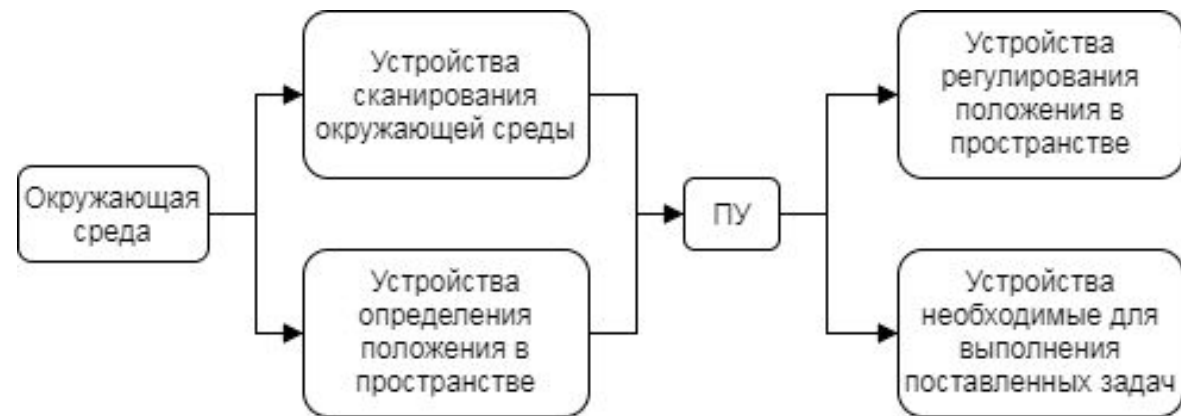
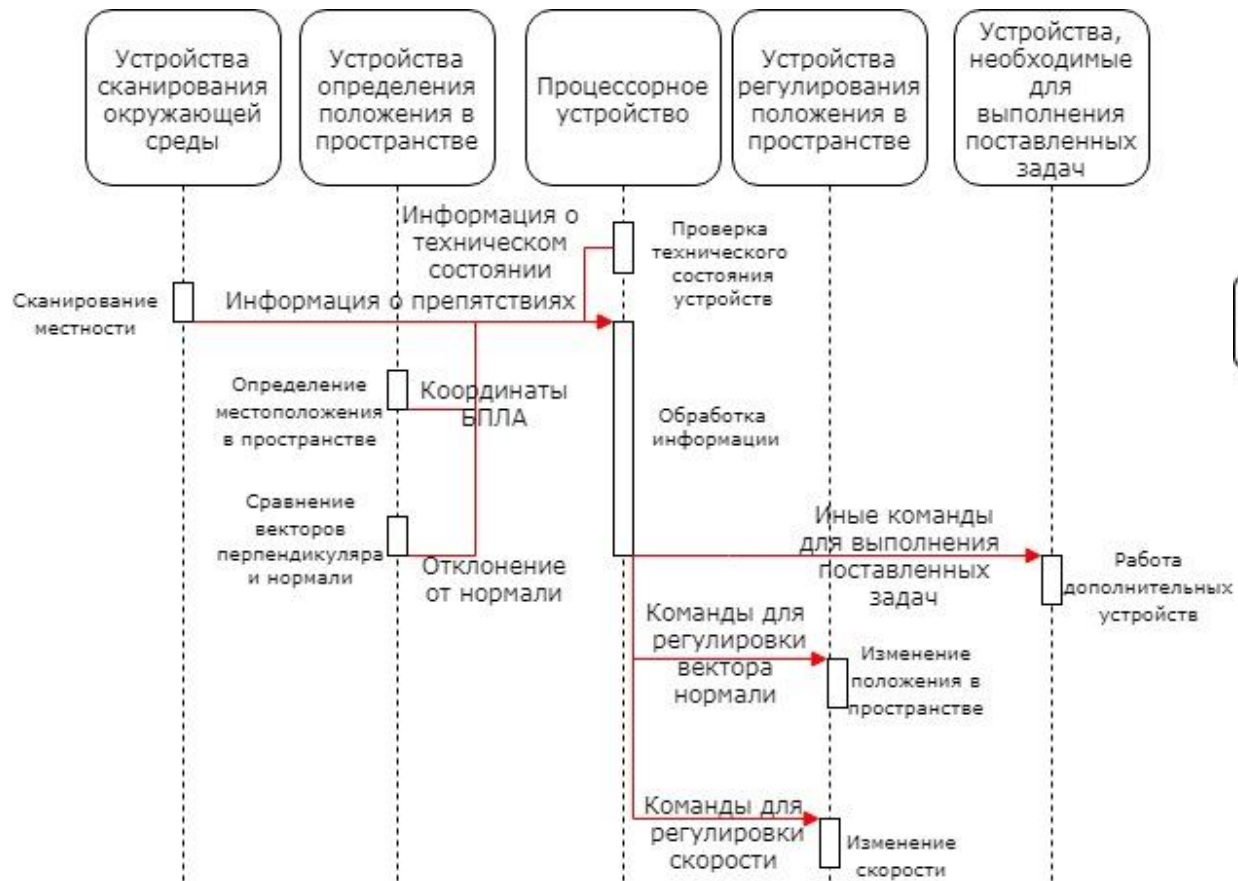
## ВНУТРЕННЕЕ ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ



## ВНЕШНЕЕ ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ



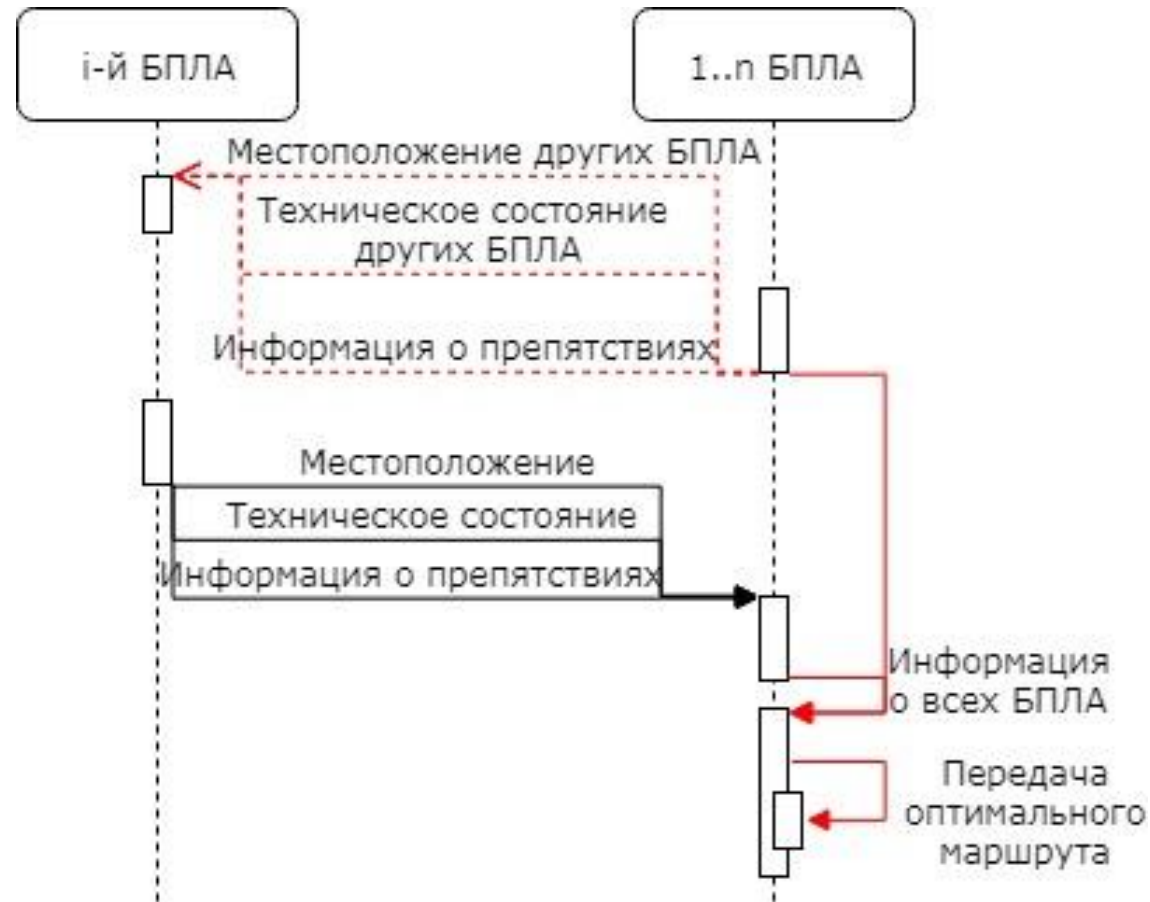
## УЯЗВИМЫЕ ИНФОРМАЦИОННЫЕ СООБЩЕНИЯ И ПРОЦЕССЫ В МОДЕЛИ ВНУТРЕННЕГО ИВ



Представление внутреннего ИВ в виде цепочки информационных сообщений

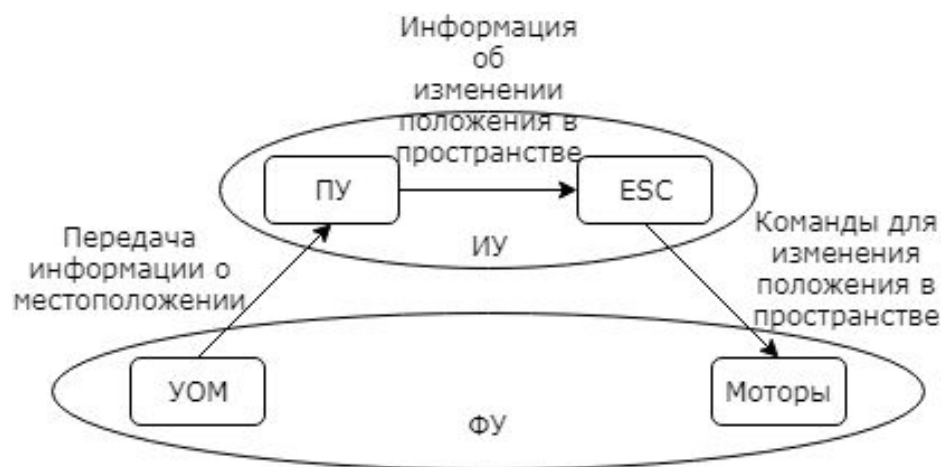


## УЯЗВИМЫЕ ИНФОРМАЦИОННЫЕ СООБЩЕНИЯ И ПРОЦЕССЫ В МОДЕЛИ ВНЕШНЕГО ИВ

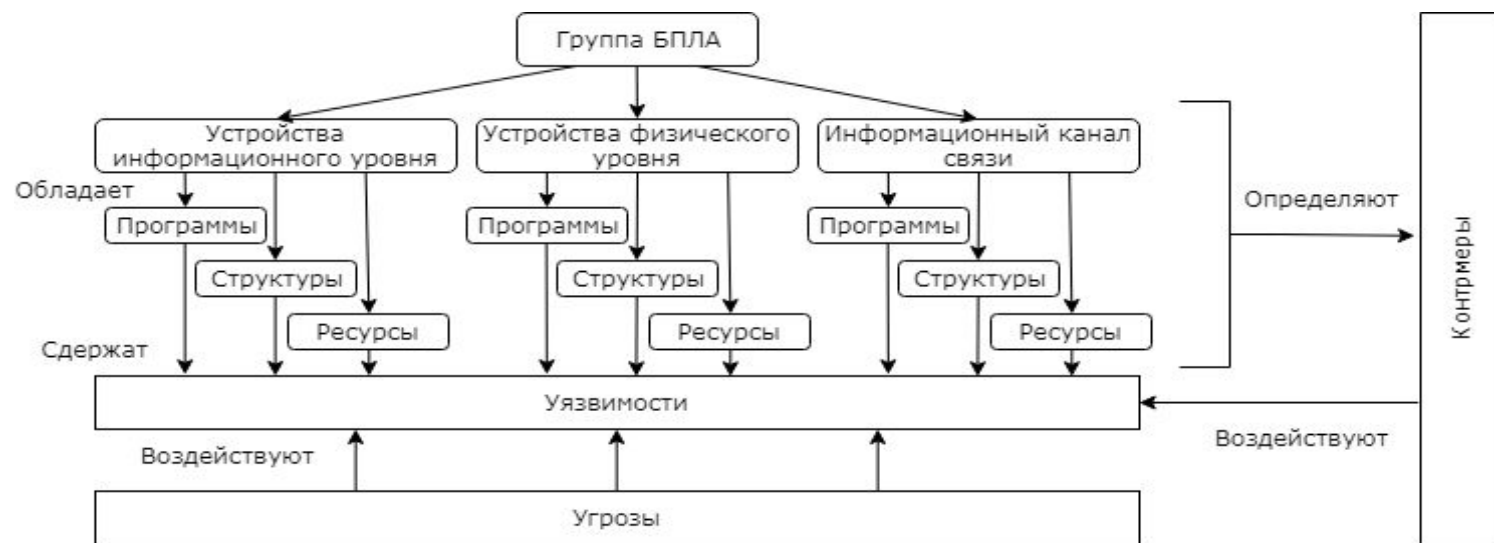


## МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОНОМНОЙ САМООРГАНИЗУЮЩЕЙСЯ ГРУППЫ БПЛА

Устройства **физического уровня (ФУ)** подчиняются командам устройств **информационного уровня (ИУ)**



Взаимодействие устройств информационного и физического уровней



## МЕТОД КЛАССИФИКАЦИИ ИНФОРМАЦИИ

Кодирование передаваемой информации  
Электронная подпись

R (read) – вывод информации  
W (write) – изменение информации  
X (execute) – выполнение

	File_1	File_2	File_3
A	R	RWX	R
B	RW	RWX	W
C	W	R	RW

## МОБИЛЬНАЯ КРИПТОГРАФИЯ

Кодирование передаваемой информации

Выполнение на стороне «клиента»



$P(E(F))$

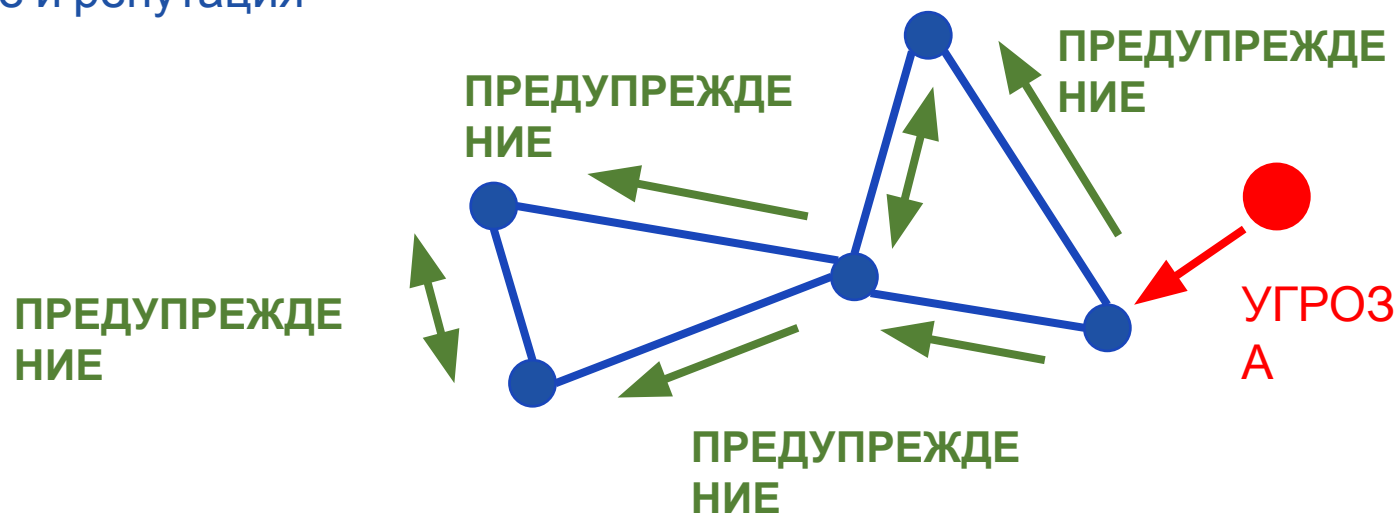
$P(E(F(I)))$



1. Шифрование функции
2. Передача программы
3. Выполнение программы
4. Передача программы
5. Дешифрация функции

## «ТОВАРИЩЕСКАЯ» МОДЕЛЬ

Передача зашифрованной информации о состоянии и угрозах  
Электронная подпись  
Доверие и репутация

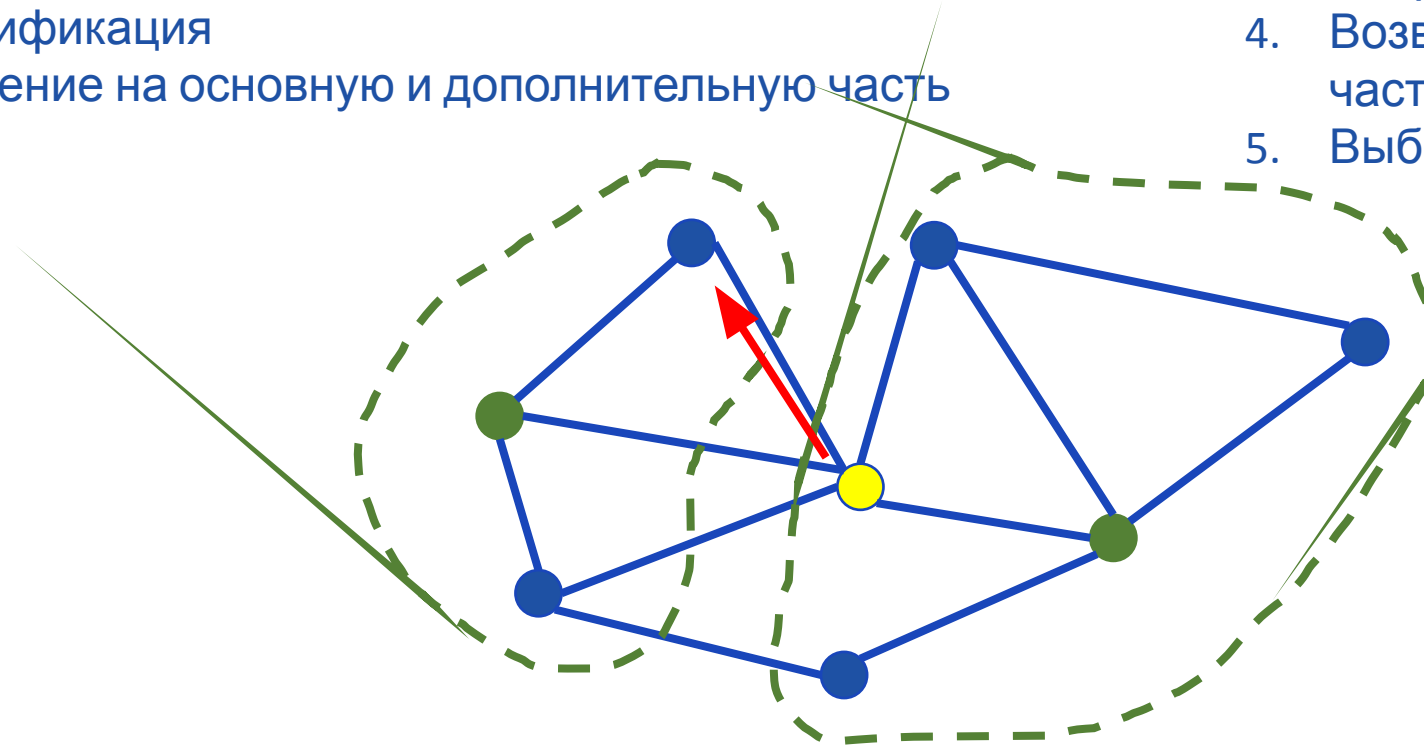


## POLICE OFFICE MODEL

Аутентификация

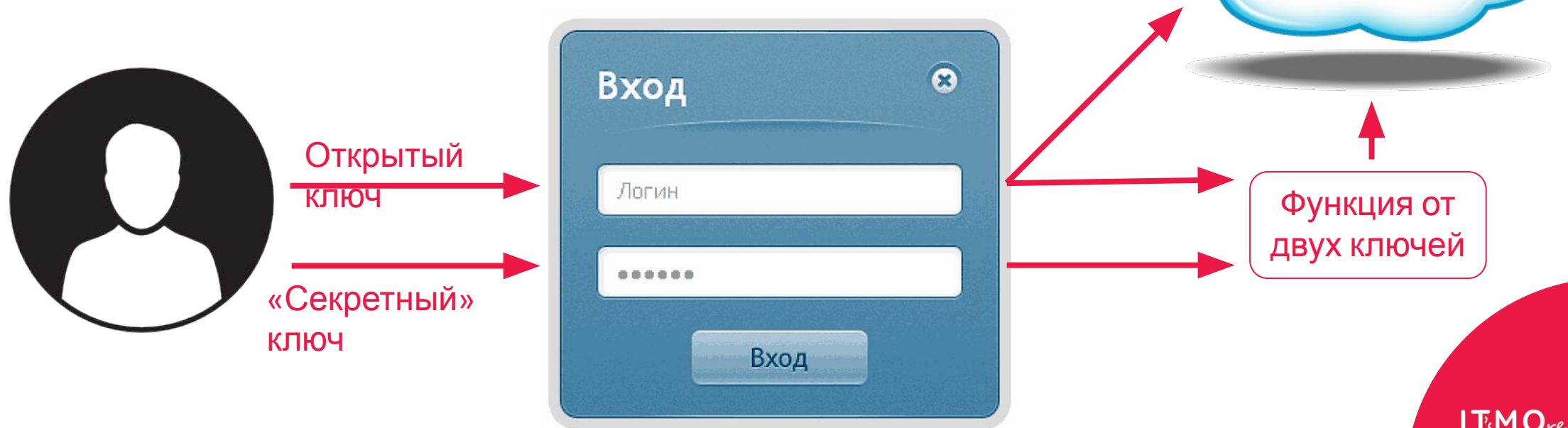
Разделение на основную и дополнительную часть

1. Выбор нового узла
2. Разделение на дополнительную и общую информацию
3. Миграция дополнительной части
4. Возвращение дополнительной части
5. Выбор дальнейшей операции

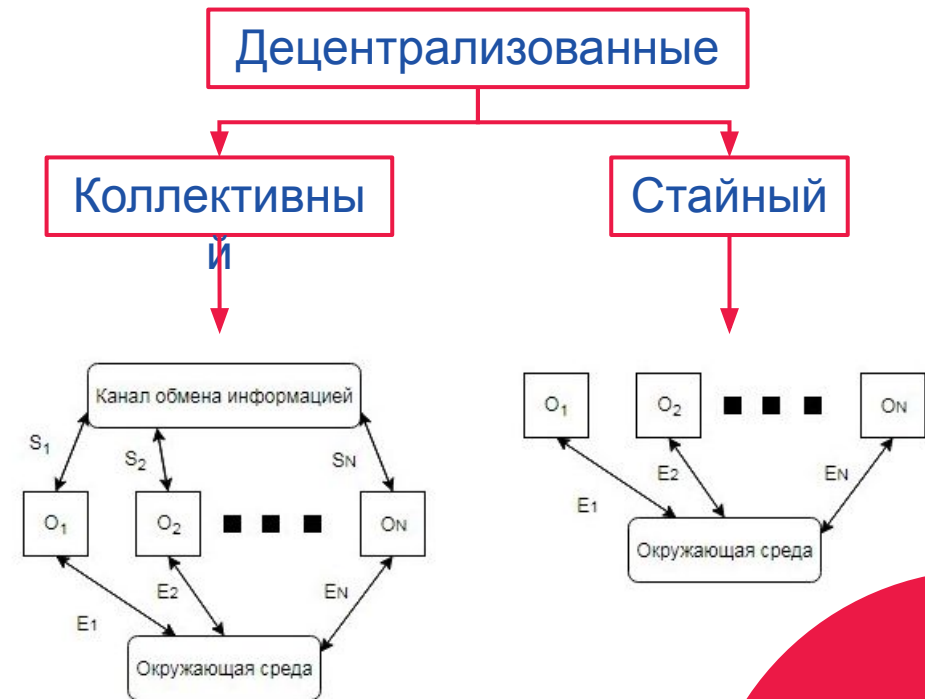
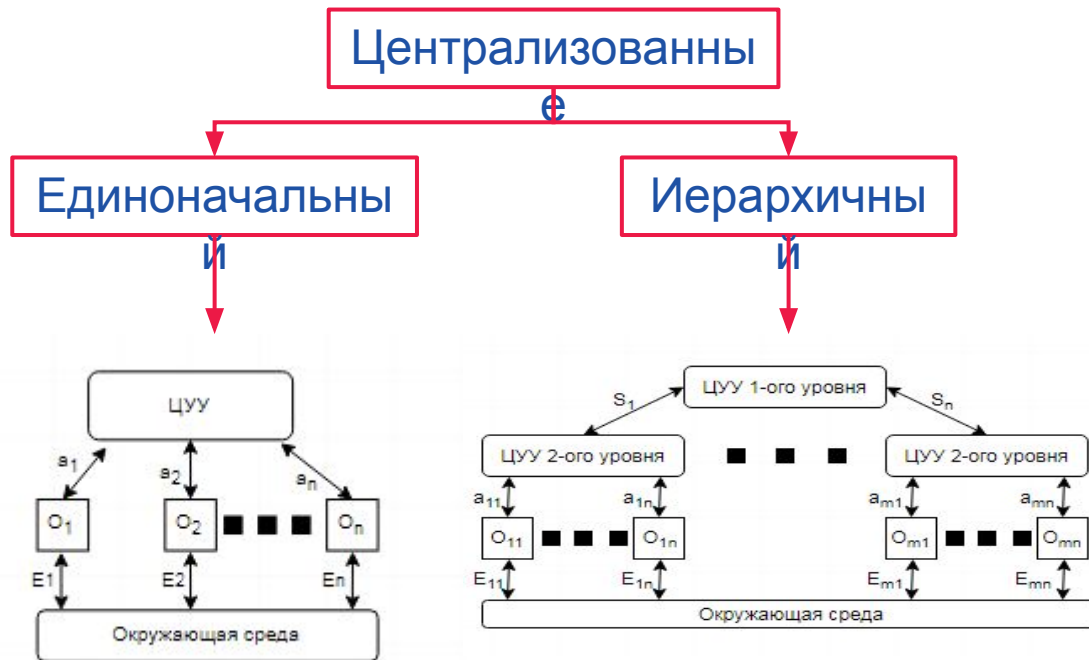


## КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ

Открытая информация  
«Секретная» информация



## МЕТОДЫ ГРУППОВОГО УПРАВЛЕНИЯ

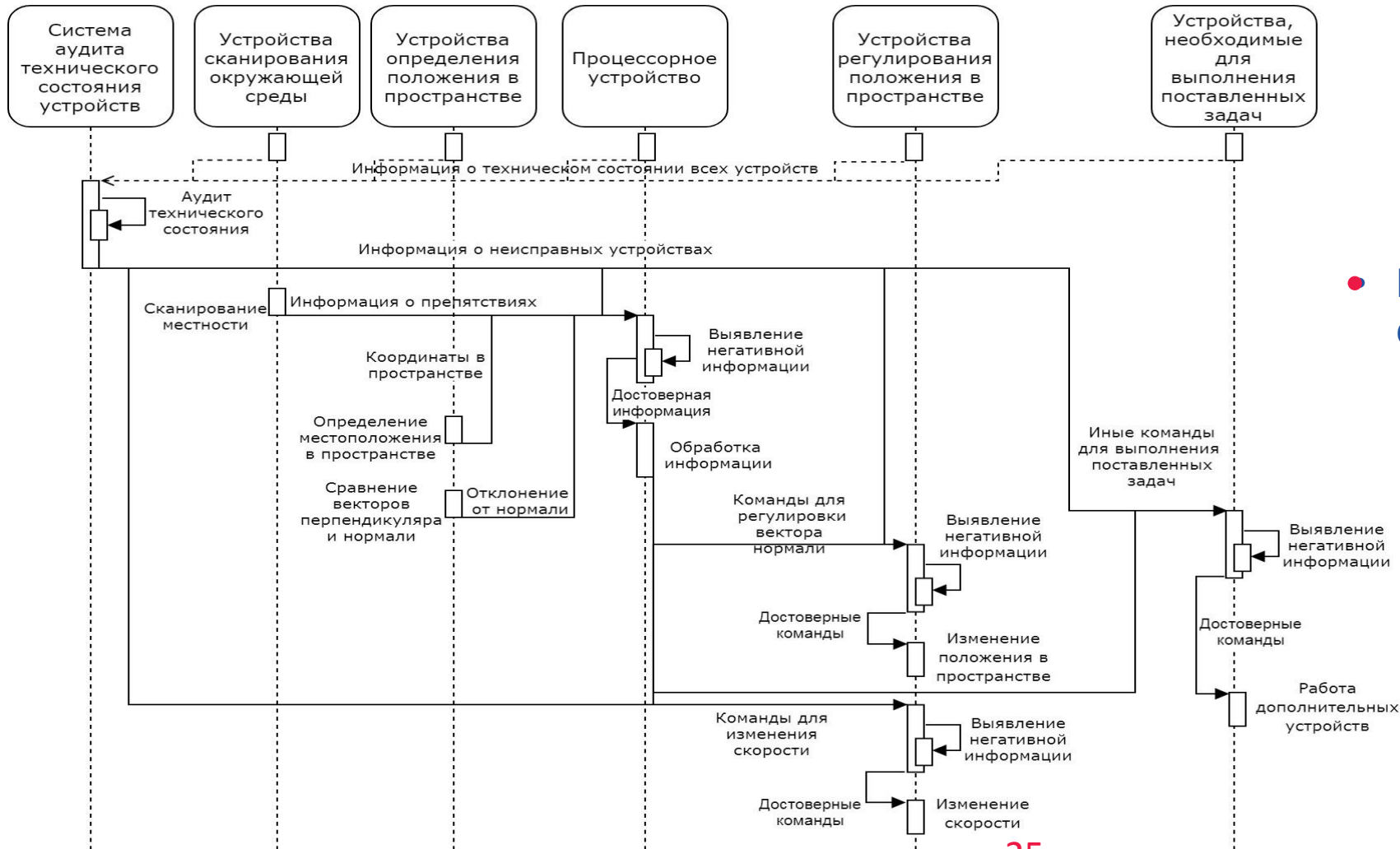




## СРАВНЕНИЕ МЕТОДОВ ГРУППОВОГО УПРАВЛЕНИЯ

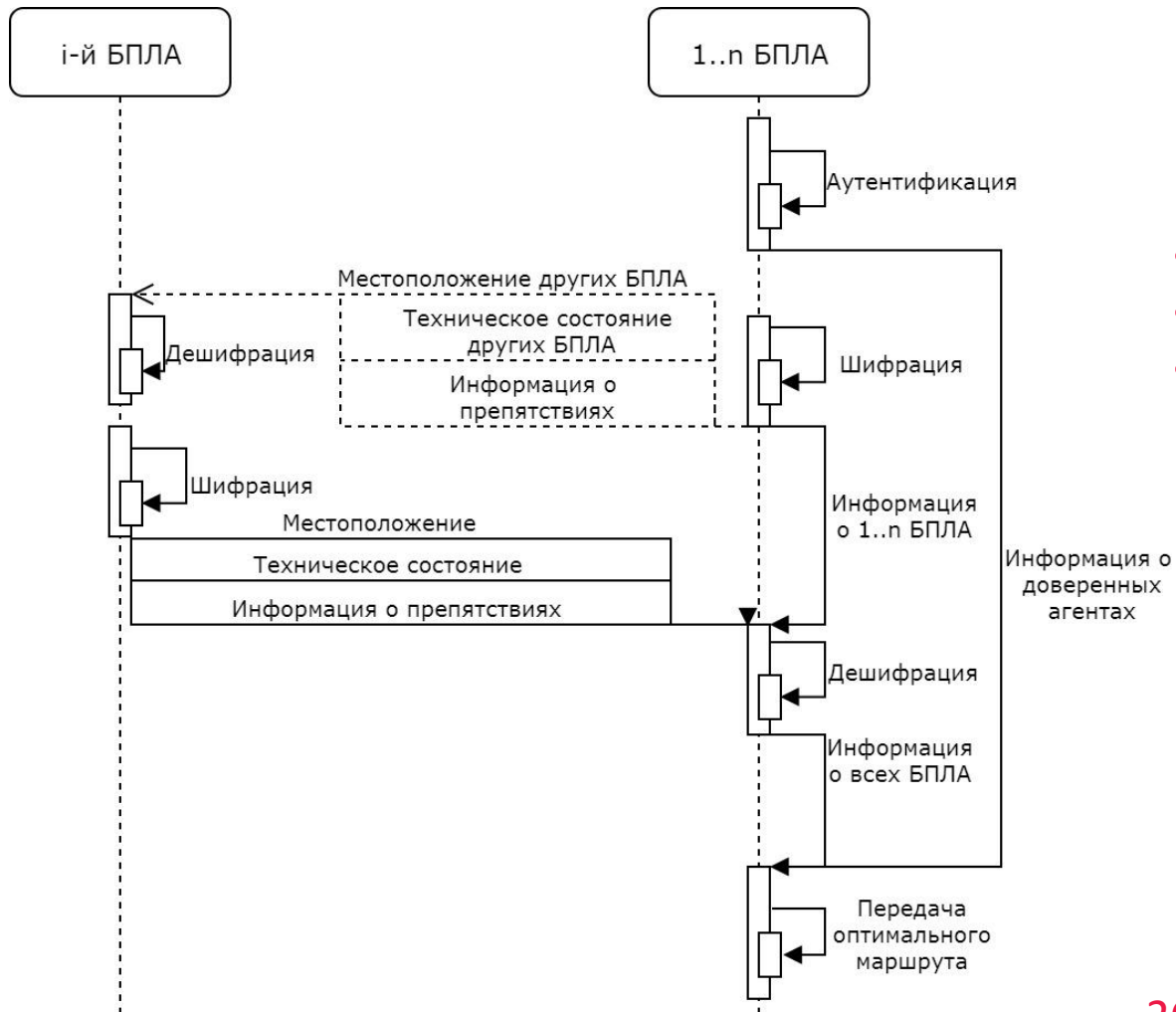
Критерии сравнения \ Названия методов	Единоначальн ый метод	Иерархичны й метод	Коллективны й метод	Стайны й метод
Структура системы	Простая	Сложная	Простая	Простая
Сложность алгоритмизации	Простая	Простая	Сложная	Сложна я
Сложность задач объектов системы	Сложная	Средняя	Сложная	Простая
Скорость принятия решений	Средняя	Низкая	Высокая	Высокая
Жизнеспособность системы	Низкая	Низкая	Высокая	Высокая
Устойчивость к угрозам со стороны ИБ	Низкая	Низкая	Средняя	Высокая
Возможность оптимизации коллективных действий коллаборации в реальном времени	Нет	Нет	Да	Нет

## МОДЕЛЬ БЕЗОПАСНОГО ВНУТРЕННЕГО ИВ



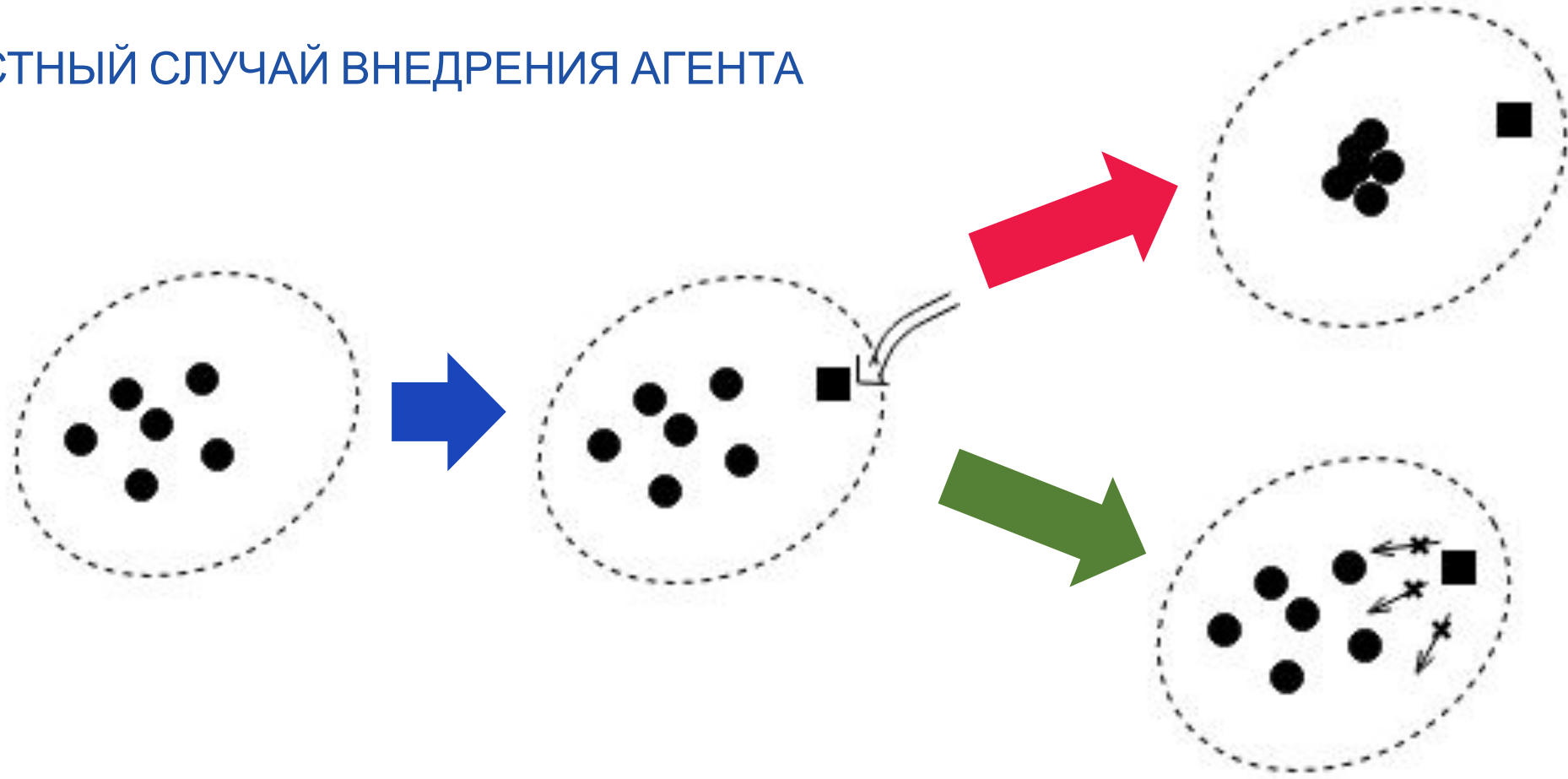
- Веден аудит технического состояния

## МОДЕЛЬ БЕЗОПАСНОГО ВНЕШНЕГО ИВ

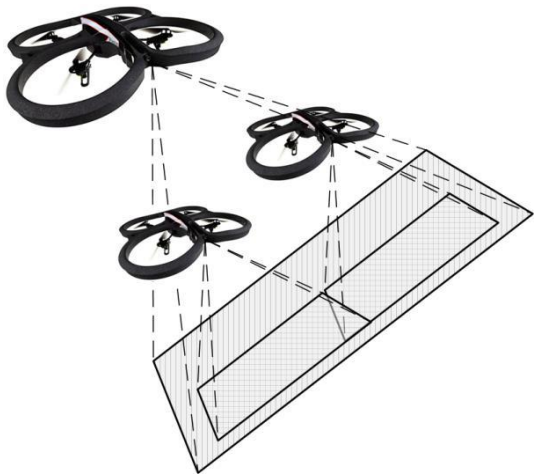


- Применена модернизированная Police Office Model
- Введена мобильная криптография
- Применена криптосистема с открытым ключом

ЧАСТНЫЙ СЛУЧАЙ ВНЕДРЕНИЯ АГЕНТА



## MULTIAGENT SYSTEMS



wixnin@mail.ru – научный руководитель лаборатории  
egormarinenkov@niuitmo.ru – ответственный за БПЛА

## ЛИТЕРАТУРА

1. Бирюков А. Информационная безопасность: защита и нападение. – Litres, 2017.
2. Konheim A. G. Computer security and cryptography. – John Wiley & Sons, 2007.
3. Молдовян Н. А. Введение в криптосистемы с открытым ключом. – БХВ-Петербург, 2005.
4. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации //М.: Горячая линия-телеком. – 2004. – Т. 16.
5. Митник К. Призрак в Сети. Мемуары величайшего хакера.

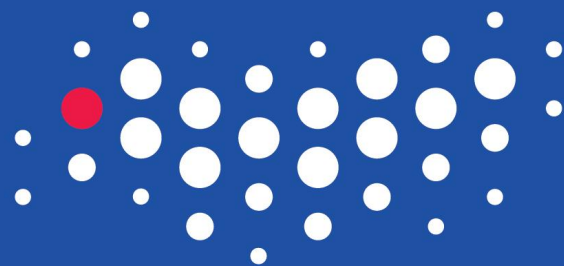
## ВОПРОСЫ

6. Информационное взаимодействие – это:
  - a) процесс дешифрации информации, с целью нарушения конфиденциальности;
  - b) процесс авторизации в системе;
  - c) процесс обмена информацией, с целью ее изменения или использования;
  
7. Уязвимость – это:
  - a) критерий, характеризующий возможность нанесения вреда системе;
  - b) критерий, характеризующий защищенность системы;
  - c) критерий, характеризующий опасность угрозы;
  
8. Что определяется программами, структурами, ресурсами системы для воздействия на уязвимости?
  - a) Угрозы;
  - b) Информационное взаимодействие;
  - c) Контрмеры;

## ВОПРОСЫ

9. Какой подход (метод) к обеспечению ИБ можно описать, как: «Выполнение зашифрованной функции на стороне «клиента», использующей его («клиента») информацию»?
  - а) «Товарищеская» модель;
  - б) Мобильная криптография;
  - с) Police Office Model;
10. Расположите стратегии группового управления в порядке убывания, сравнивая их по критерию устойчивости к угрозам (первая – высокая, второй – средняя, третий – низкая).
  - а) Централизованная единоначальная;
  - б) Децентрализованная стайная;
  - с) Децентрализованная коллективная;





# УНИВЕРСИТЕТ ИТМО

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: MR. ROBOT В РЕАЛИЯХ РОССИЙСКОГО УНИВЕРСИТЕТА

ДОКЛАДЧИК:

МАРИНЕНКОВ ЕГОР ДЕНИСОВИЧ

КОВАЛЕНКО АЛЕКСАНДР ВАЛЕРЬЕВИЧ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

САНКТ-ПЕТЕРБУРГ