Адаптивная обманная система для рефлексивного управления злоумышленником

Лаврова Дарья

План доклада

Конфликт ИБ

- Выбор математического аппарата для формализации
- Формализация конфликта ИБ

Рефлексивное управление противником в конфликте

- Выбор механизма реализации рефлексивного управления
- Обобщенная модель угроз безопасности ИС
- Выбор стратегий рефлексивного управления

Концепция адаптивной обманной системой для рефлексивного управления злоумышленником

- Объекты-ловушки ИС
- Максимизация длины графа действий злоумышленника в обманной системе

Необходимость формализации конфликта ИБ

Конфликт ИБ - неразрешимый двусторонний конфликт между администратором безопасности и злоумышленником, предметом которого является безопасность информационной системы

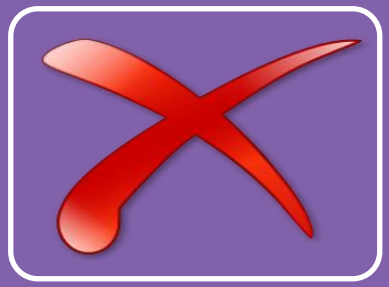
Математическое описание поведения противоборствующих сторон в конфликте

Математическое описание возможных стратегий поведения злоумышленника

Варианты развития стратегий

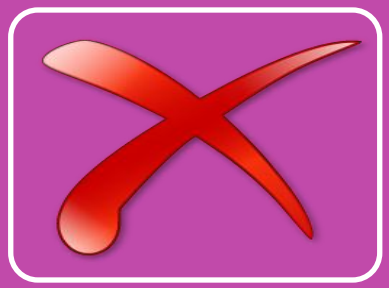
Возможность расширения функционала механизмов защиты

Выбор математического аппарата для формализации конфликта ИБ



Ланчестеровские модели

- В начальном состоянии конфликта каждая сторона имеет полную информацию о силах и средствах своего противника



Теория игр

- Теория игр исходит из принципа минимума среднего риска, что неприемлемо для конфликта ИБ

Алгебра конфликтов Лефевра

- Возможность имитации рассуждений противоборствующих сторон
- Возможность описания рефлексивного управления

Формализация конфликта информационной безопасности

Администратор безопасности А	S - инфраструктура защищаемой ИС (плацдарм)	Злоумышленник Н
S_A - представление А о плацдарме S		S_H - представление Н о плацдарме S
I_A – цель А (обеспечение ИБ защищаемой системы)		I_H – цель Н (нарушение ИБ целевой системы)
D_A – доктрина А (комплекс мер и действий для обеспечения ИБ)		D_H – доктрина Н (совокупность действий и средств для нарушения ИБ)
R_A – решение задачи обеспечения ИБ системы		R_H – решение задачи нарушения ИБ системы

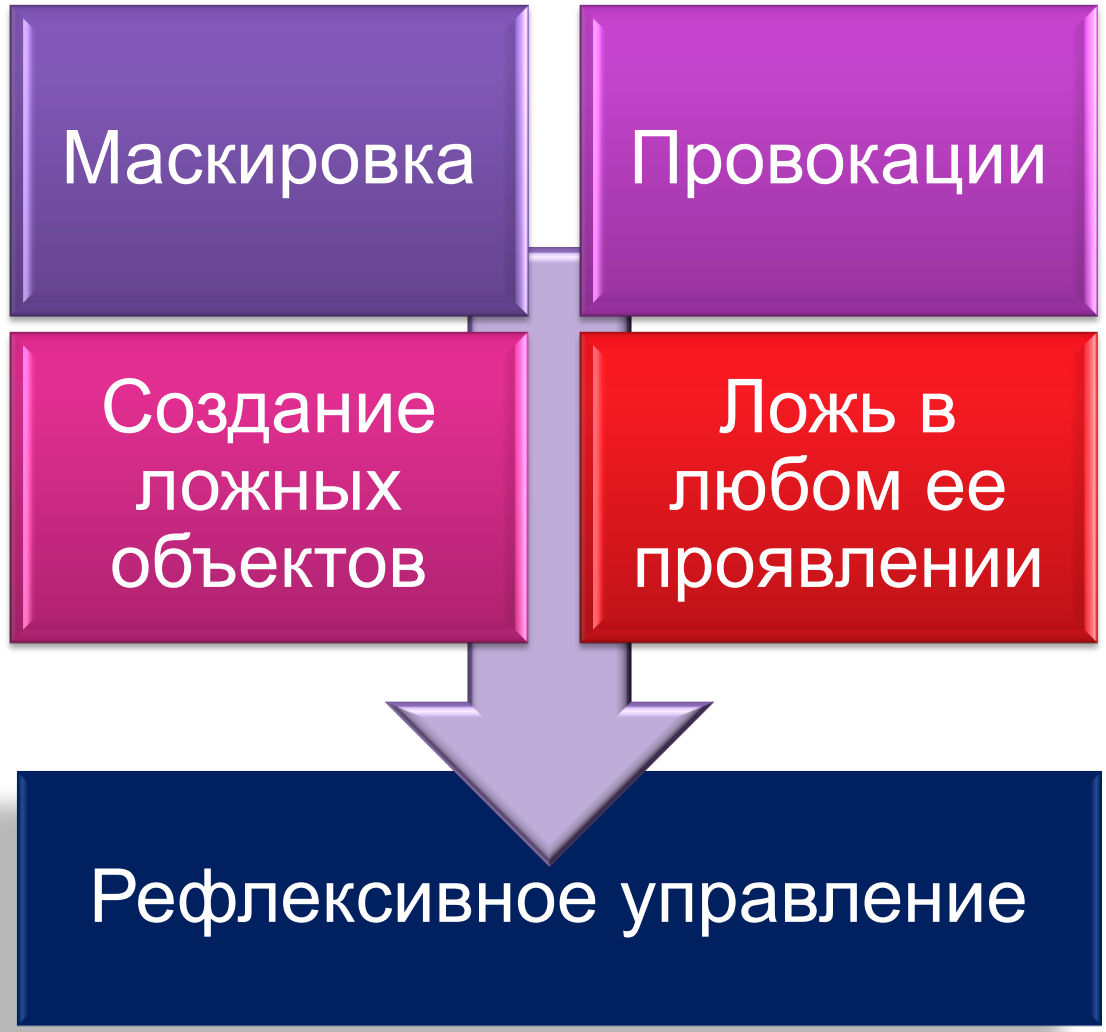
$$\frac{I_A}{S_A} D_A \rightarrow \frac{R_A}{S_A}$$

$$\frac{I_{AH}}{S_{AH}} D_{AH} \rightarrow \frac{R_{AH}}{S_{AH}}$$

$$\frac{R_{AH}}{S_H} \rightarrow \frac{R_{AH} I_H}{S_H} D_H \rightarrow \frac{R_H}{S_H}$$

$$\frac{I_{AH}}{S_{AH}} D_{AH} \rightarrow \frac{R_{AH}}{S_{AH}} \rightarrow \frac{R_{AH}}{S_H} \rightarrow \frac{R_{AH} I_H}{S_H} D_H \rightarrow \frac{R_H}{S_H}$$

Рефлексивное управление



Реализация рефлексивного управления:

- Передача противнику оснований для принятия решения
- Управление решением противника
- Навязывание противнику определенной линии поведения

Стратегии рефлексивного управления противником

Рефлексивное управление посредством передачи ложной информации о плацдарме

$S_{HA} \rightarrow S_H$

Рефлексивное управление посредством формирования цели противника

$I_{HA} \rightarrow I_H$

Рефлексивное управление посредством формирования доктрины противника

$D_{HA} \rightarrow D_H$

Рефлексивное управление посредством передачи решения

$R_{HA} \rightarrow R_H$

Формирование цели посредством передачи картины плацдарма

$I_{HA} \rightarrow S_{HA} \rightarrow S_H \rightarrow I_H$

Рефлексивное управление посредством превращения:

$S_{HAH} \rightarrow S_{HA}$

$I_{HAH} \rightarrow I_{HA}$

$D_{HAH} \rightarrow D_{HA}$

Рефлексивное управление посредством цепочки

$I_{HAH} \rightarrow S_{HAH} \rightarrow S_{HA} \rightarrow I_{HA}$

Нейтрализация дедукции противника

Обманные системы как инструмент реализации стратегии рефлексивного управления

Имитация реальной системы

↓

Введение злоумышленника в заблуждение

↓

Сокрытие и маскировка информационных ресурсов

↓

Снижение оперативности и результативности действий злоумышленника

↓

Реализация рефлексивного управления

Угрозы безопасности информационной системы

Физический уровень

- Встраивание аппаратных закладок
- Выведение из строя компонентов ИС
- Уничтожение физических носителей информации
- Внедрение в линии связи
- Использование фото и видеоаппаратуры

Сетевой уровень

- Нарушение доступности оборудования
- Перехват сетевого трафика
- Модификация сетевого трафика

Уровень ОС

- Установка ВПО
- Нарушение стабильности работы системных процессов и служб
- Воздействие на информационные ресурсы (копирование, редактирование, удаление информации)

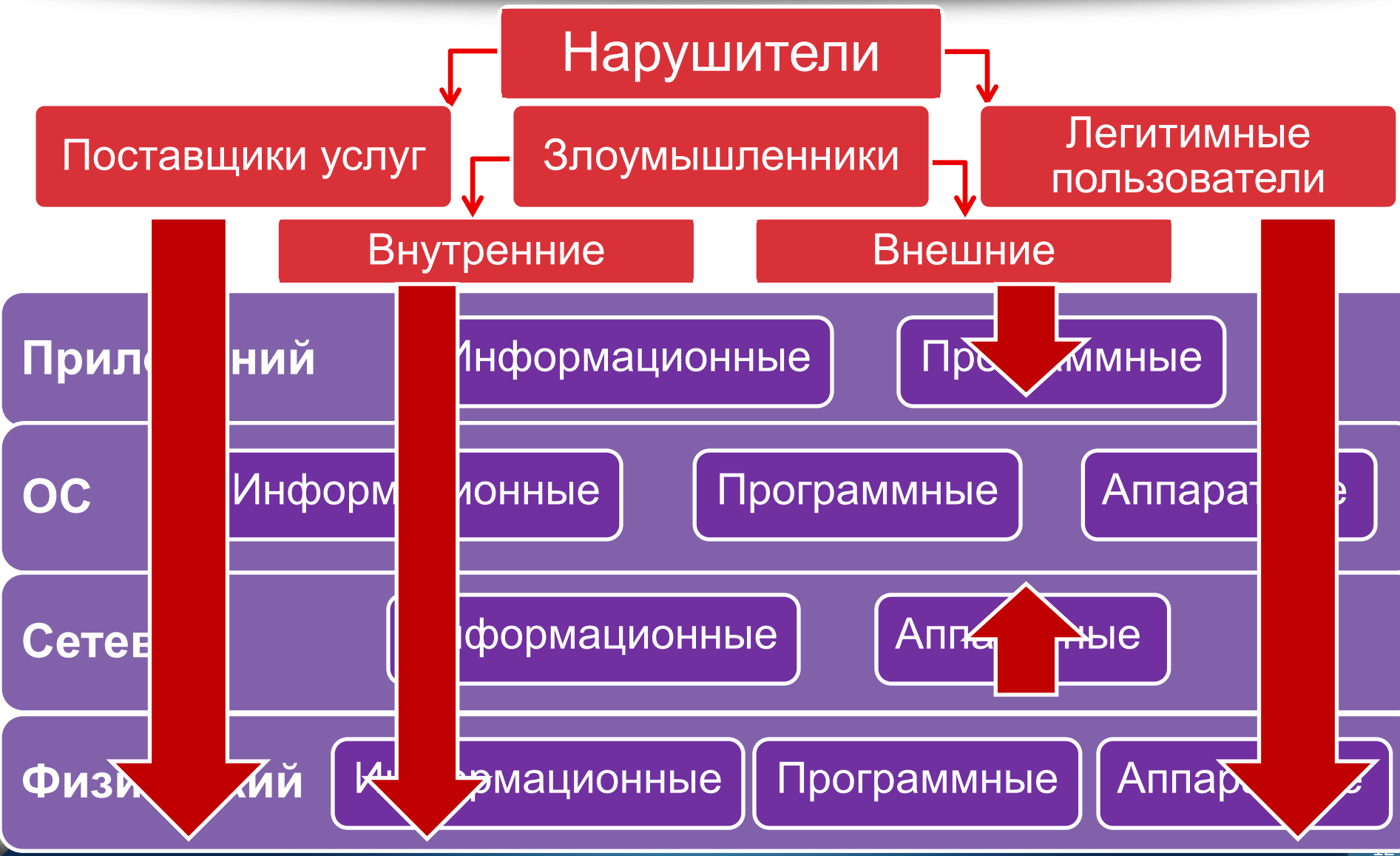
Уровень приложений

- Вывод из строя приложений
- Воздействие на информационные ресурсы приложений
- Модификации функционирования приложений

Критические объекты информационной системы

Аппаратные	• Компьютеры • Сетевое оборудование • Физические носители информации
Программные	• Службы и процессы ОС • Программные приложения
Информационные ресурсы	• Сетевой трафик • Файлы • Информация из БД • Письма • Логины/пароли

Обобщенная модель угроз безопасности ИС



Выбор стратегий рефлексивного управления для реализации в обманных системах

- Стратегия передачи ложной информации о плацдарме
- Стратегия рефлексивного управления посредством формирования цели противника
- Стратегия формирования цели посредством передачи картины плацдарма
- Стратегия рефлексивного управления посредством превращения $S_{НАН} \rightarrow S_{НА}$
- Стратегия рефлексивного управления посредством цепочки $I_{НАН} \rightarrow S_{НАН} \rightarrow S_{НА} \rightarrow I_{НА}$

Объекты-«ловушки» информационной системы

Уровень сети

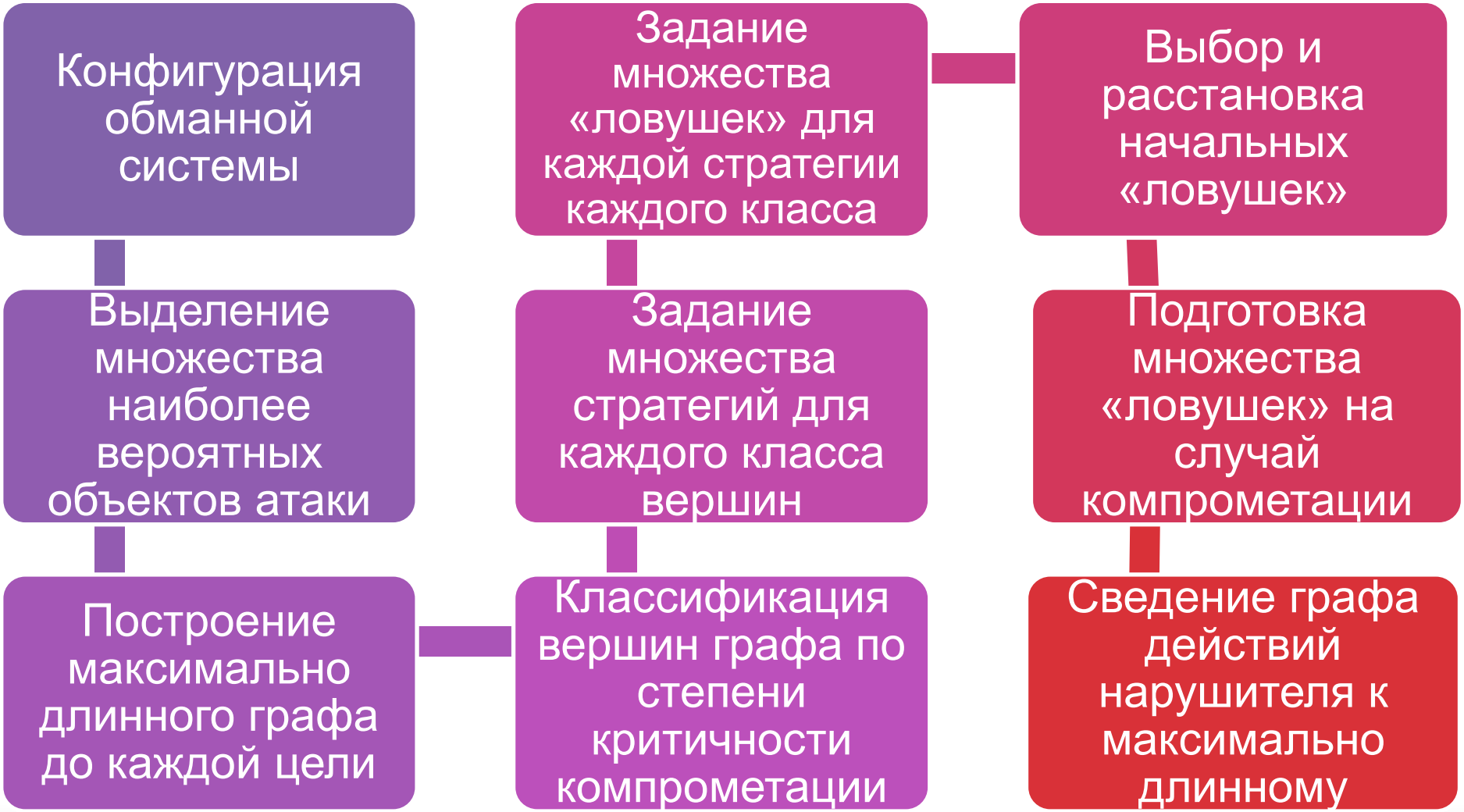
- Сетевой протокол
- Сетевой трафик
- Хост
- Открытые порты

Уровни ОС и приложений

- ОС
- Сервисы и ПО
- Уязвимости
- Файлы

Стратегия рефлексивного управления	Пример используемых «ловушек»
Передачи ложной информации о плацдарме	Открытые порты Хост Сетевой протокол
Рефлексивного управления посредством формирования цели противника	Сетевой трафик Открытые порты ОС Сервисы и ПО Уязвимости
Формирования цели посредством передачи картины плацдарма	Сетевой трафик Открытые порты Уязвимости Файлы
Рефлексивного управления посредством превращения	Сетевой трафик Файлы
Рефлексивного управления посредством цепочки	Сетевой трафик Файлы

Концепция адаптивной обманной системы



Описание примера обманной системы

Конфигурация обманной системы

- 9 компьютеров
- Файловый сервер
- Компьютер администратора
- Защищаемый сервер

Цели

- Файловый сервер
- Защищаемый сервер
- Компьютер администратора

Критичность компрометации

- Файловый сервер - низкая
- 9 компьютеров – средняя
- Компьютер администратора, защищаемый сервер - высокая

Стратегии и «ловушки» примера обманной системы

Низкая критичность компрометации

Превращения

- Ложная документация

Средняя критичность компрометации

Ложной информации о плацдарме

- Открытые порты

Рефлексивного управления посредством формирования цели

- Открытые порты
- Уязвимости

Высокая критичность компрометации

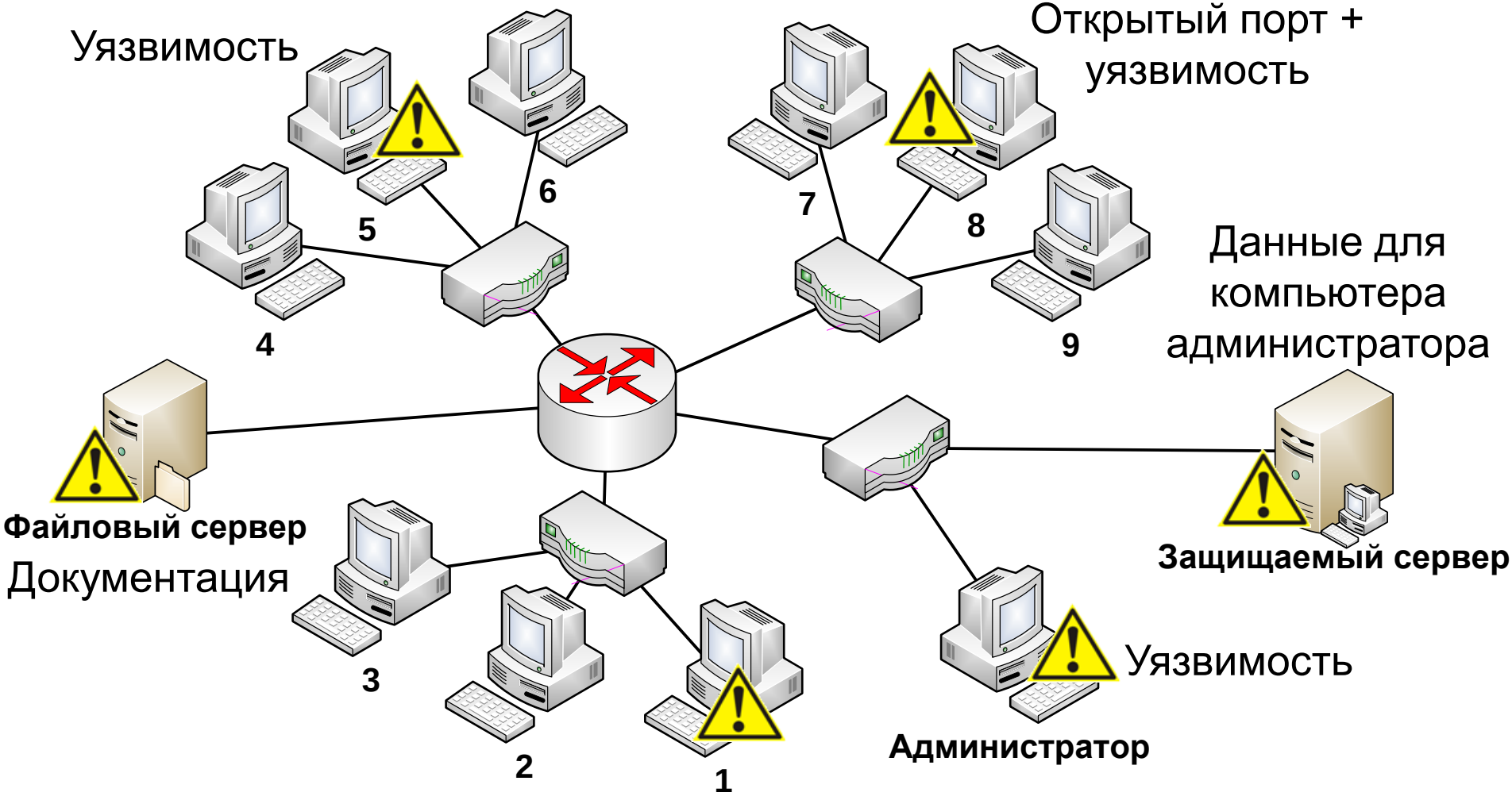
Рефлексивного управления посредством цепочки

- Файлы (письма)

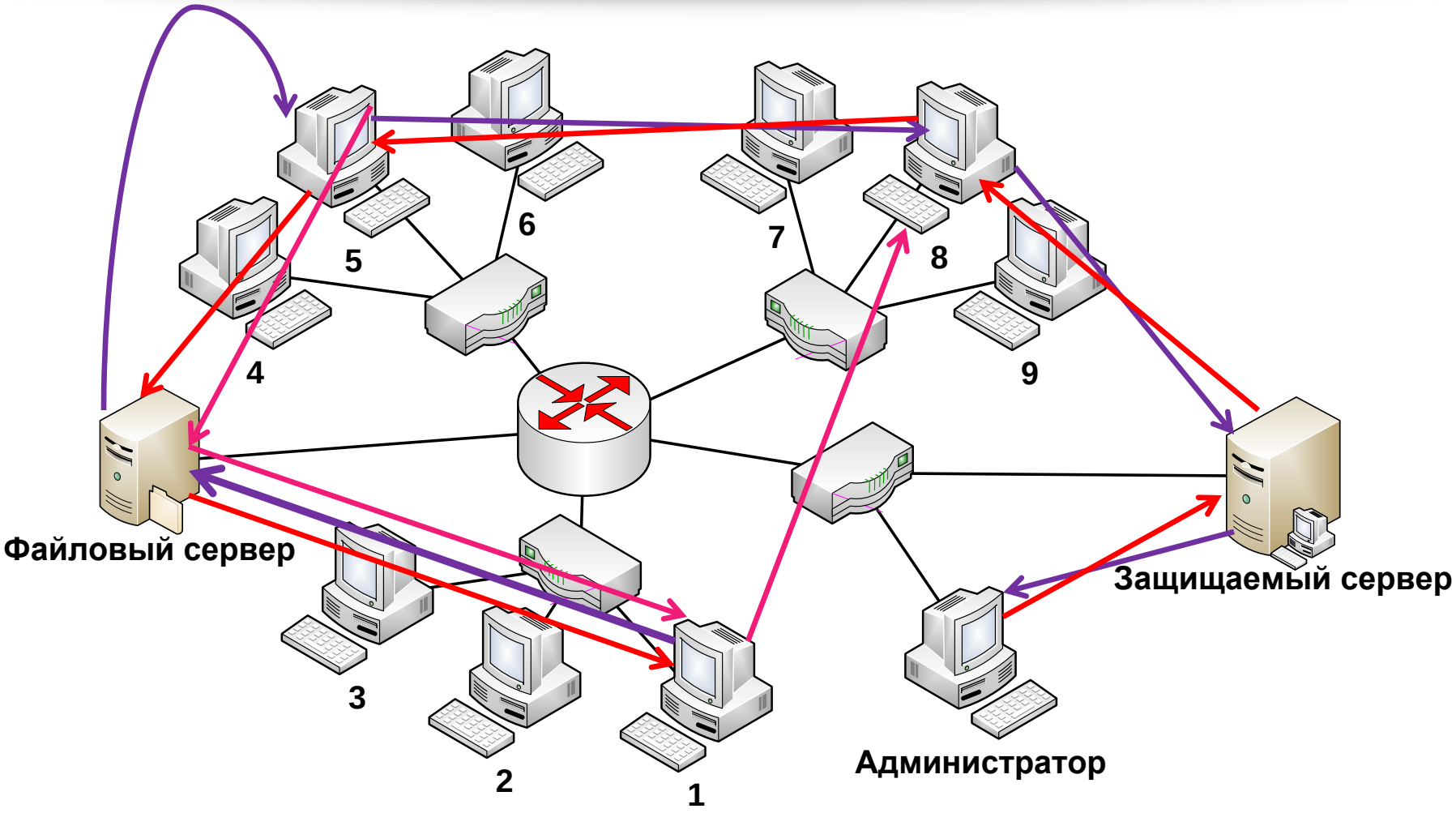
Формирования цели посредством передачи картины плацдарма

- Файлы

Пример конфигурации обманной системы



Адаптивная обманная система



Спасибо за внимание!