КАФЕДРА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ»

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Адаптивное управление безопасностью информационных систем, построенных на базе программно-конфигурируемых сетей

Павленко Евгений Юрьевич

ОСОБЕННОСТИ СОВРЕМЕННЫХ ПОДХОДОВ К АНАЛИЗУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **ВАРИАТИВНОСТЬ ПРЕДЛАГАЕМЫХ МЕТОДОВ ОБНАРУЖЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
- **КАЖДОЕ СРЕДСТВО ОБНАРУЖЕНИЯ НАРУШЕНИЙ ФУНКЦИОНИРУЕТ НА ОДНОМ-ДВУХ УРОВНЯХ СИСТЕМЫ**
- **ОТСУТСТВУЕТ ВЗАИМОДЕЙСТВИЕ МЕЖДУ СРЕДСТВАМИ ОБНАРУЖЕНИЯ НАРУШЕНИЙ, ФУНКЦИОНИРУЮЩИМИ НА РАЗНЫХ УРОВНЯХ СИСТЕМЫ**

АНАЛИЗ МЕТОДОВ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННОГО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (ВПО) (1)

УРОВЕНЬ ПРИЛОЖЕНИЙ ОПЕРАЦИОННОЙ СИСТЕМЫ

ОСОБЕННОСТИ МЕХАНИЗМОВ ДЕЙСТВИЯ ВПО	ОСОБЕННОСТИ МАСКИРОВКИ	ВОЗМОЖНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ
❖ ИСПОЛЬЗОВАНИЕ СИСТЕМ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ, ЭЛЕКТРОННОЙ ПОЧТЫ В КАЧЕСТВЕ КАНАЛА РАСПРОСТРАНЕНИЯ; ❖ ФИШИНГ, ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ В ПОПУЛЯРНЫХ ПРИЛОЖЕНИЯХ ❖ ПОДДЕРЖКА СВЯЗИ С КОМАНДНЫМИ СЕРВЕРАМИ ❖ ВНЕДРЕНИЕ В ДРУГИЕ ПРОЦЕССЫ	❖ ОБФУСКАЦИЯ КОДА ❖ ПОЛИМОРФИЗМ, ШИФРОВАНИЕ КОДА ❖ ИСПОЛЬЗОВАНИЕ АНОНИМНЫХ СЕТЕЙ ❖ ИСПОЛЬЗОВАНИЕ ИКОНОК ИЗВЕСТНЫХ ПРИЛОЖЕНИЙ ❖ ИМИТАЦИЯ ЛЕГИТИМНОГО ФУНКЦИОНАЛА ❖ ИСПОЛЬЗОВАНИЕ ЛОГИЧЕСКИХ БОМБ	❖ СИГНАТУРНЫЙ АНАЛИЗ, ❖ ЭВРИСТИЧЕСКИЙ АНАЛИЗ, ❖ ВЫПОЛНЕНИЕ ПРОГРАММЫ В ПЕСОЧНИЦЕ ❖ РЕПУТАЦИОННЫЙ МЕТОД ОБНАРУЖЕНИЯ ❖ WHITELISTING, BLACKLISTING ❖ АНАЛИЗ СЕТЕВОГО ТРАФИКА ❖ КОНТРОЛЬ ЦЕЛОСТНОСТИ ФАЙЛОВ

АНАЛИЗ МЕТОДОВ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННОГО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (ВПО) (2)

УРОВЕНЬ ЯДРА ОПЕРАЦИОННОЙ СИСТЕМЫ

ОСОБЕННОСТИ МЕХАНИЗМОВ ДЕЙСТВИЯ ВПО	ОСОБЕННОСТИ МАСКИРОВКИ	ВОЗМОЖНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ
❖ ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ ОС ❖ ИЗМЕНЕНИЕ СИСТЕМНЫХ ОБЪЕКТОВ ❖ ВНЕДРЕНИЕ СОБСТВЕННЫХ ДРАЙВЕРОВ ❖ МАНИПУЛИРОВАНИЕ С ДАННЫМИ НА СИСТЕМНОМ УРОВНЕ	❖ ОБФУСКАЦИЯ КОДА ❖ ШИФРОВАНИЕ КОДА ❖ ИСПОЛЬЗОВАНИЕ РУТКИТНЫХ ТЕХНИК ДЛЯ СКРЫТИЯ СВОИХ ФАЙЛОВ, ПРОЦЕССОВ ❖ ОБНАРУЖЕНИЕ ВИРТУАЛЬНОГО ОКРУЖЕНИЯ ❖ КОМПРОМЕТАЦИЯ СЕРТИФИКАТОВ ДЛЯ ПОДПИСИ ДРАЙВЕРОВ	❖ АНАЛИЗ СЕТЕВОГО ТРАФИКА ❖ СИГНАТУРНЫЙ АНАЛИЗ ❖ ИССЛЕДОВАНИЕ ПАМЯТИ ❖ СКАНИРОВАНИЕ ТАБЛИЦ ДЕСКРИПТОРОВ ПРЕРЫВАНИЙ И ДИСПЕТЧЕРИЗАЦИИ СИСТЕМНЫХ СЛУЖБ ❖ СРАВНЕНИЕ ДАННЫХ ИЗ РАЗЛИЧНЫХ ИСТОЧНИКОВ ❖ КОНТРОЛЬ ЦЕЛОСТНОСТИ ЯДРА ОС

АНАЛИЗ МЕТОДОВ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННОГО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (ВПО) (3)

УРОВЕНЬ ГИПЕРВИЗОРА

ОСОБЕННОСТИ МЕХАНИЗМОВ ДЕЙСТВИЯ ВПО	ОСОБЕННОСТИ МАСКИРОВКИ	ВОЗМОЖНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ
❖ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ И РЕЖИМА СИСТЕМНОГО УПРАВЛЕНИЯ ❖ ВОЗМОЖНОСТЬ ПЕРЕХВАТА СОБЫТИЙ БОЛЕЕ ВЫСОКОГО УРОВНЯ ❖ МОГУТ БЫТЬ РЕАЛИЗОВАНЫ В ВИДЕ ДРАЙВЕРА ❖ КОНТРОЛЬ ФУНКЦИОНИРОВАНИЯ ОС	❖ ИЗМЕНЕНИЕ СКОРОСТИ РАБОТЫ ТАЙМЕРОВ И СЧЕТЧИКА ТАКТОВ ДЛЯ ВИРТУАЛЬНОЙ МАШИНЫ ❖ ВОЗДЕЙСТВИЕ НА СРЕДСТВА ОБНАРУЖЕНИЯ ВПО	❖ СИГНАТУРНЫЙ АНАЛИЗ ❖ АНАЛИЗ ВРЕМЕННЫХ ЗАДЕРЖЕК ❖ ПОВЕДЕНЧЕСКИЙ АНАЛИЗ ❖ ИССЛЕДОВАНИЕ ИДЕНТИФИКАТОРОВ ВИРТУАЛЬНЫХ УСТРОЙСТВ ❖ СКАНИРОВАНИЕ ПРОЦЕССОВ

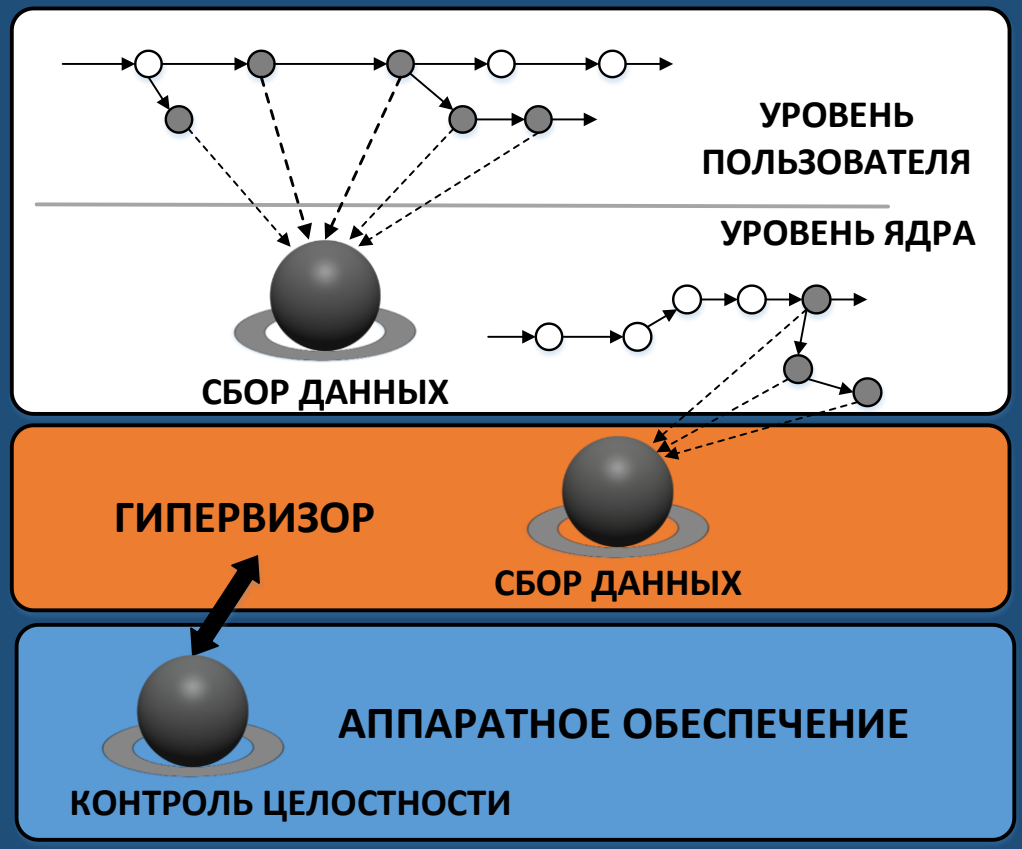
АНАЛИЗ МЕТОДОВ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННОГО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (ВПО) (4)

УРОВЕНЬ АППАРАТНОГО ОБЕСПЕЧЕНИЯ

ОСОБЕННОСТИ МЕХАНИЗМОВ ДЕЙСТВИЯ ВПО	ОСОБЕННОСТИ МАСКИРОВКИ	ВОЗМОЖНЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ
❖ ИСПОЛЬЗОВАНИЕ АРХИТЕКТУРНЫХ УЯЗВИМОСТЕЙ И УЯЗВИМОСТЕЙ МИКРОПРОГРАММ, УПРАВЛЯЮЩИХ АППАРАТНЫМ ОБЕСПЕЧЕНИЕМ ❖ НАРУШЕНИЕ ЛОГИКИ РАБОТЫ АППАРАТНЫХ КОМПОНЕНТОВ	❖ БЛОКИРОВКА ПОПЫТОК ОБНОВЛЕНИЯ ПРОШИВКИ ❖ ИСПОЛЬЗОВАНИЕ РУТКИТ-МЕХАНИЗМОВ ❖ ИСПОЛЬЗОВАНИЕ ОБЛАСТЕЙ, НЕДОСТУПНЫХ ДЛЯ ТРАДИЦИОННЫХ СРЕДСТВ ЗАЩИТЫ	❖ ОТСЛЕЖИВАНИЕ ПОТОКА ИНФОРМАЦИИ В ЛОГИЧЕСКИХ ЭЛЕМЕНТАХ ПРОЦЕССОРА ❖ СРАВНЕНИЕ ФИНАЛЬНОГО ИЗДЕЛИЯ И ОБРАЗЦА ❖ ДЕСТРУКТИВНОЕ ТЕСТИРОВАНИЕ ❖ ФАЗЗИНГ

ИЕРАРХИЧЕСКИЙ ПОДХОД К АНАЛИЗУ БЕЗОПАСНОСТИ

ПРОБЛЕМА СУЩЕСТВУЮЩИХ ПОДХОДОВ – ОТСУТСТВИЕ СОГЛАСОВАННОСТИ И ОБОСОБЛЕННОСТЬ СУЩЕСТВУЮЩИХ СРЕДСТВ ЗАЩИТЫ, ФУНКЦИОНИРУЮЩИХ НА РАЗЛИЧНЫХ УРОВНЯХ.
ЭТО ПОЗВОЛЯЕТ ВПО ЗАДЕЙСТВОВАТЬ КОМПОНЕНТЫ РАЗНЫХ УРОВНЕЙ И МАНИПУЛИРОВАТЬ ДАННЫМИ ДЛЯ ОБХОДА МЕХАНИЗМОВ АНАЛИЗА И КОНТРОЛЯ БЕЗОПАСНОСТИ

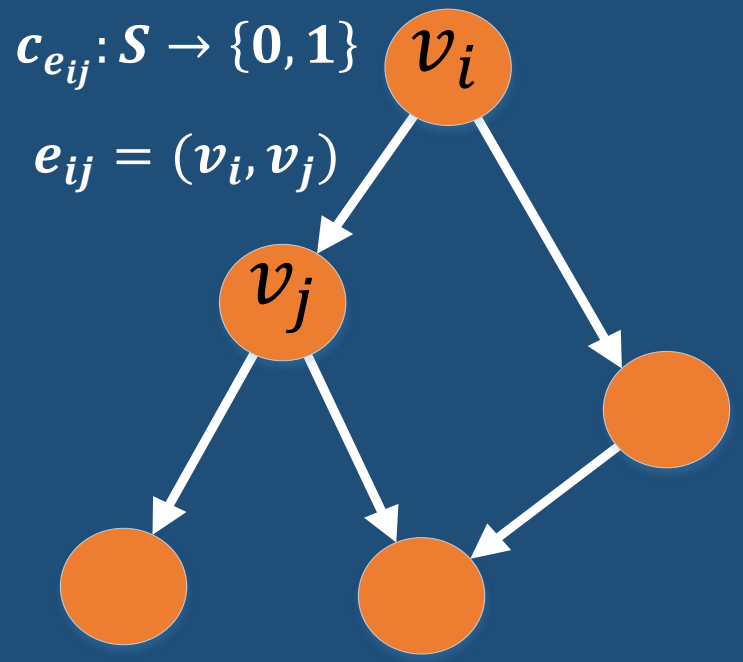


ИСПОЛЬЗОВАНИЕ ВПО ТОЛЬКО НА НИЗКИХ УРОВНЯХ НЕ ИСПОЛЬЗУЕТСЯ НАРУШИТЕЛЯМИ

ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ЦЕЛЕВОЙ ИНФОРМАЦИИ НЕОБХОДИМЫ КОМПОНЕНТЫ НА УРОВНЕ ПРИЛОЖЕНИЙ (В КРАЙНЕМ СЛУЧАЕ, НА УРОВНЕ ЯДРА ОС)

ИЕРАРХИЧЕСКАЯ ГРАФОВО-СОБЫТИЙНАЯ МОДЕЛЬ МЕЖКОМПОНЕНТНОГО ВЗАИМОДЕЙТВИЯ

СОБЫТИЙНАЯ МОДЕЛЬ $M =< V, E, S, F, C, P >$:

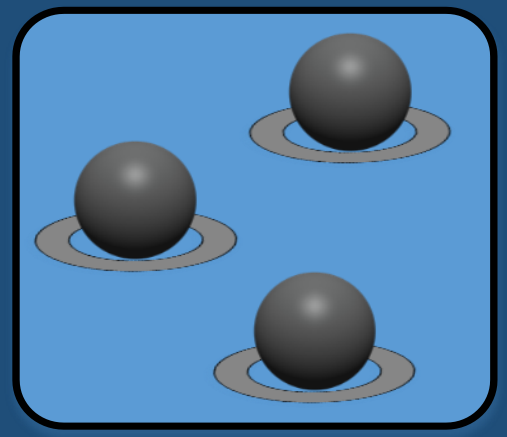


- КАЖДОЕ СОБЫТИЕ ХАРАКТЕРИЗУЕТСЯ КОРТЕЖЕМ $< id, type, source, A_{type} >$

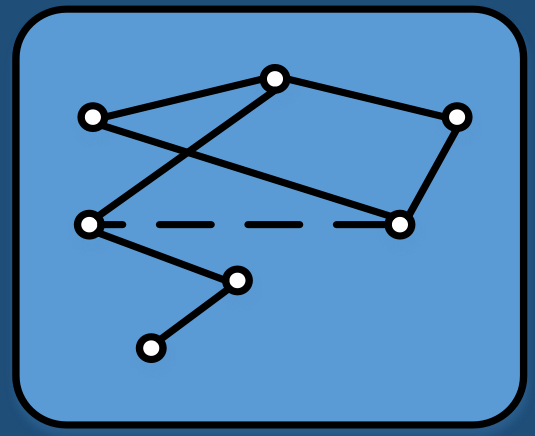
- V - МНОЖЕСТВО ВЕРШИН ГРАФА, ХАРАКТЕРИЗУЕТ МНОЖЕСТВО СОБЫТИЙ
- E - МНОЖЕСТВО РЕБЕР ГРАФА, ХАРАКТЕРИЗУЕТ ПЕРЕХОДЫ $e_{ij} = (v_i, v_j)$, ЗАДАЕТ ВЗАИМОСВЯЗЬ СОБЫТИЙ v_i И v_j
- МНОЖЕСТВО СОСТОЯНИЙ СИСТЕМЫ $S = (s_1, s_2, \dots, s_k)$
- МНОЖЕСТВО ФУНКЦИЙ ИЗМЕНЕНИЯ СОСТОЯНИЙ СИСТЕМЫ $F = \{f_{v_i}: S \to S \mid \forall\, v_i \in V\}$
- МНОЖЕСТВО ЛОГИЧЕСКИХ УСЛОВИЙ, АССОЦИИРОВАННЫХ С ПЕРЕХОДАМИ МЕЖДУ СОБЫТИЯМИ $C = \{c_{e_{ij}}: S \to \{0,1\} \mid \forall\, e_{ij} \in E\}$
- $P = \{P_{v_i}: S \to B \mid \forall\, v_i \in V\}$ НАБОР ГРАНИЧНЫХ УСЛОВИЙ, ЗАДАЮЩИХ НЕБЕЗОПАСНОЕ СОСТОЯНИЕ $B \subset S$

СХЕМА РАБОТЫ ПРЕДЛАГАЕМОГО ПОДХОДА

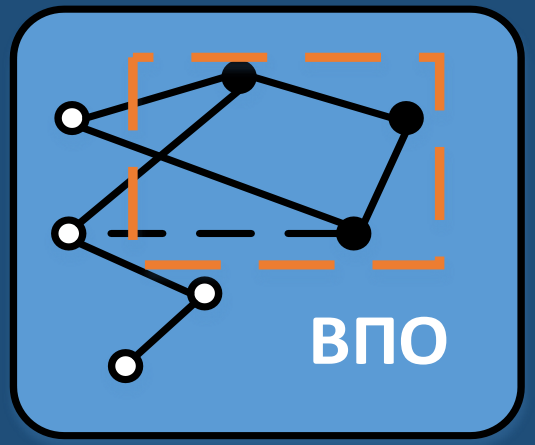
СБОР ДАННЫХ



ПОСТРОЕНИЕ СОБЫТИЙНОГО ГРАФА



АНАЛИЗ И ПРИНЯТИЕ РЕШЕНИЯ



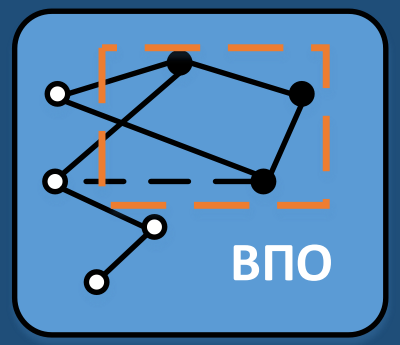
ПОЛУЧЕННАЯ ИНФОРМАЦИЯ ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ СВЯЗЕЙ МЕЖДУ СОБЫТИЯМИ

НА ОСНОВЕ СВЯЗЕЙ ГЕНЕРИРУЕТСЯ ГРАФ СОБЫТИЙ ПРОГРАММЫ, ХАРАКТЕРИЗУЮЩИЙ ЕЕ ПОВЕДЕНИЕ

ИЗВЛЕЧЕНИЕ ИНФОРМАЦИОННЫХ ХАРАКТЕРИСТИК, НЕОБХОДИМЫХ ДЛЯ ПРИНЯТИЯ РЕШЕНИЯ О ТОМ, ЯВЛЯЕТСЯ ПРОГРАММА ВРЕДОНОСНОЙ ИЛИ НЕТ

СПОСОБЫ ОПРЕДЕЛЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АНАЛИЗ И ПРИНЯТИЕ РЕШЕНИЯ



ИСПОЛЬЗОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ВПО:

ОЦЕНКА ПОДОБИЯ ГРАФОВ ВРЕДОНОСНОЙ И ИССЛЕДУЕМОЙ ПРОГРАММ G_1 И G_2

ПОИСК МАКСИМАЛЬНОГО ОБЩЕГО ПОДГРАФА $MCS(G_1, G_2)$

$$\Delta(G_1, G_2) = 1 - \frac{|MCS(G_1, G_2)|}{|G_1| + |G_2| - |MCS(G_1, G_2)|}$$

ПОИСК МИНИМАЛЬНОГО ОБЩЕГО НАДГРАФА $mcs(G_1, G_2)$

$$\Delta(G_1, G_2) = |mcs(G_1, G_2)| - |MCS(G_1, G_2)|$$

ВЫЧИСЛЕНИЕ РАССТОЯНИЯ (ЗНАЧЕНИЕ ОТ 0 ДО 1, ДЛЯ ИЗОМОРФНЫХ ГРАФОВ ПРИНИМАЕТ ЗНАЧЕНИЕ 0)

$$\Delta(G_1, G_2) = 1 - \frac{|MCS(G_1, G_2)|}{max\{|G_1|, |G_2|\}}$$

ПОДХОД К АДАПТИВНОМУ УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ ГОМЕОСТАЗА

ГОМЕОСТАЗ КАК СВОЙСТВО БЕЗОПАСНОСТИ: СПОСОБНОСТЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЕСПЕЧИВАТЬ НЕОБХОДИМОЕ ЗНАЧЕНИЕ ОБЪЕМА ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПУТЕМ ВНЕСЕНИЯ АРХИТЕКТУРНЫХ ИЗМЕНЕНИЙ В ОТВЕТ НА ДЕСТРУКТИВНОЕ ВОЗДЕЙСТВИЕ

СВОЙСТВА ДЛЯ ОЦЕНКИ СПОСОБНОСТИ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ К ГОМЕОСТАЗУ:

ВЕКТОР $x_i(t) = \{x_{i_1}(t), x_{i_2}(t), \dots, x_{i_k}(t)\}$ **ПАРАМЕТРОВ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ** — ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ КАЖДОГО КОМПОНЕНТА РИС, С УЧЕТОМ ТЕКУЩИХ НАСТРОЕК В ДАННЫЙ МОМЕНТ ВРЕМЕНИ, ГДЕ i – КОЛИЧЕСТВО КОМПОНЕНТОВ РИС, А k – КОЛИЧЕСТВО ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ДЛЯ КОМПОНЕНТА ДАННОГО ТИПА. ОБЛАСТЬ ДОПУСТИМЫХ ЗНАЧЕНИЙ ПЕРЕМЕННЫХ $x_i(t)$ ОПРЕДЕЛЯЕТСЯ ТИПОМ И СЛОЖНОСТЬЮ КОМПОНЕНТА

ВЕКТОР $A_i(t) = \{A_{i_1}(t), A_{i_2}(t), \dots, A_{i_k}(t)\}$ **ПАРАМЕТРОВ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ** — ОПРЕДЕЛЯЮЩИХ СИЛУ АТАКУЮЩЕГО ВОЗДЕЙСТВИЯ НА ПАРАМЕТРЫ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ i-ОГО КОМПОНЕНТА РИС В ДАННЫЙ МОМЕНТ ВРЕМЕНИ

ВЕКТОР $M_i(t) = \{M_{i_1}(t), M_{i_2}(t), \dots, M_{i_k}(t)\}$ **ПАРАМЕТРОВ УПРАВЛЯЮЩИХ ВОЗДЕЙСТВИЙ** — ОПРЕДЕЛЯЮЩИХ МЕРУ УПРАВЛЯЮЩЕГО ВОЗДЕЙСТВИЯ НА ПАРАМЕТРЫ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ i-ОГО КОМПОНЕНТА РИС В ДАННЫЙ МОМЕНТ ВРЕМЕНИ

СИСТЕМНЫЙ ПОДХОД К ОЦЕНКЕ СПОСОБНОСТИ СИСТЕМЫ К ГОМЕОСТАЗУ

ОБЪЕМ ФУНКЦИОНАЛЬНОГО ПРОСТРАНСТВА V_f ДЛЯ ОПРЕДЕЛЕННОГО ТИПА УСТРОЙСТВ - МАТРИЦА РАЗМЕРА k НА i, СТРОКИ КОТОРОЙ - ЗНАЧЕНИЯ ВЕКТОРА $x_i(t)$ ДЛЯ ВОЗМОЖНОСТЕЙ i-ОГО КОМПОНЕНТА РИС В ДАННЫЙ МОМЕНТ ВРЕМЕНИ

СПОСОБНОСТЬ ПАРАМЕТРОВ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ РИС К УПРАВЛЯЮЩЕМУ ВОЗДЕЙСТВИЮ:

$$W_M = \left[x_i^T * M_i\right]: W_{M_{ij}} = \begin{cases} x_i^T * M_i, & \text{ЕСЛИ } x_i^T * M_i \in \Omega_i \\ 0, & \text{ЕСЛИ } x_i * M_i \notin \Omega_i \end{cases}$$

СПОСОБНОСТЬ ПАРАМЕТРОВ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ РИС К АТАКУЮЩЕМУ ВОЗДЕЙСТВИЮ:

$$W_A = \left[x_i^T * A_i\right]: W_{A_{ij}} = \begin{cases} x_i^T * A_i, & \text{ЕСЛИ } x_i^T * A_i \in \Omega_i \\ 0, & \text{ЕСЛИ } x_i * A_i \notin \Omega_i \end{cases}$$

ДЛЯ ОПРЕДЕЛЕНИЯ СПОСОБНОСТИ РИС К ГОМЕОСТАЗУ ВЫЧИСЛЯЮТСЯ СРЕДНЕКВАДРАТИЧНЫЕ ЗНАЧЕНИЯ δ_M И δ_A КОЭФФИЦИЕНТОВ ЧУВСТВИТЕЛЬНОСТИ:

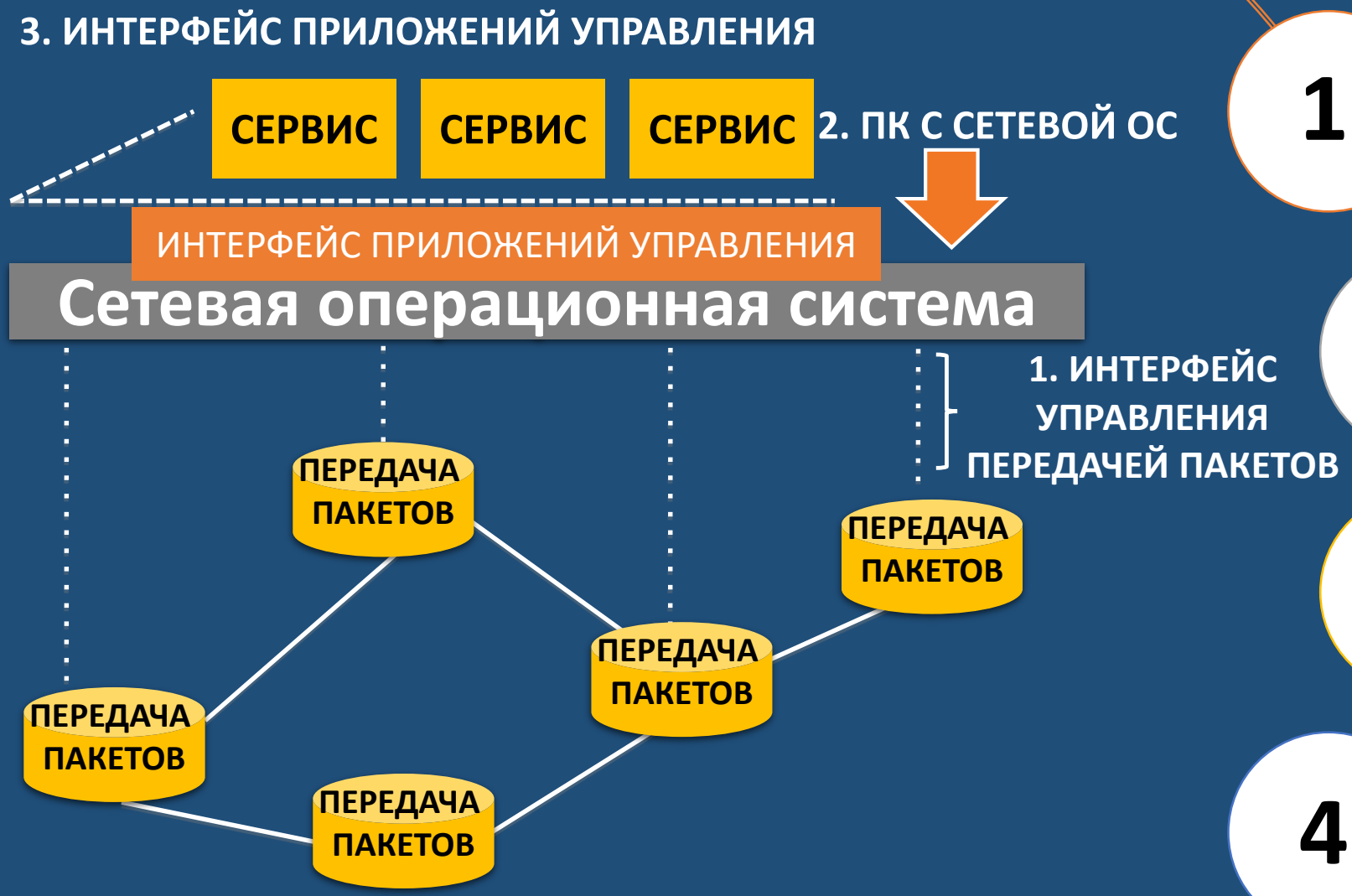
$$\delta_M^2 = \frac{1}{k^2}\sum_{i=1}^{k}\sum_{j=1}^{m} W_{M_{ij}}^2 = \frac{1}{k^2} tr(W_M * W_M^T)$$

$$\delta_A^2 = \frac{1}{k^2}\sum_{i=1}^{k}\sum_{j=1}^{m} W_{A_{ij}}^2 = \frac{1}{k^2} tr(W_A * W_A^T)$$

ЛОКАЛЬНАЯ ГОМЕОСТАТИЧЕСКАЯ СПОСОБНОСТЬ h И ЛОКАЛЬНАЯ СПОСОБНОСТЬ К АТАКУЮЩЕМУ ВОЗДЕЙСТВИЮ d РИС ОПРЕДЕЛЯЮТСЯ КАК $h = \delta_M^{-1}$ И $d = \delta_A^{-1}$

ПРОГРАММНО-КОНФИГУРИРУЕМЫЕ СЕТИ

УПРАВЛЕНИЕ НА БАЗЕ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ



1. ВОЗМОЖНОСТЬ ДИНАМИЧЕСКОГО ПЕРЕСТРОЕНИЯ МАРШРУТОВ ПЕРЕДАЧИ ДАННЫХ В ЗАВИСИМОСТИ ОТ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ
2. ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ВСЕЙ СЕТЬЮ, ДЛЯ УЧЕТА ИЗМЕНЕНИЯ ВО ВСЕХ ЭЛЕМЕНТАХ СЕТИ
3. ВОЗМОЖНОСТЬ АВТОМАТИЧЕСКОГО ПРОГРАММНОГО УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ СЕТЕВОГО ОБОРУДОВАНИЯ
4. НЕЗАВИСИМОСТЬ ОТ СПЕЦИФИЧНЫХ ХАРАКТЕРИСТИК И ВОЗМОЖНОСТЕЙ КОНКРЕТНОГО СЕТЕВОГО ОБОРУДОВАНИЯ

СПОСОБ УПРАВЛЕНИЯ СЕТЕВЫМИ ПОТОКАМИ В СИСТЕМАХ, ПОСТРОЕННЫХ НА БАЗЕ ТЕХНОЛОГИИ ПКС

ПОСТАНОВКА ЗАДАЧИ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ

$$\min_{\vec{X}} \{ f_1(\vec{X}), f_2(\vec{X}), f_3(\vec{X}), \dots, f_k(\vec{X}) \}, \vec{X} \in S$$

$$f_i: R^n \to R$$

$$\vec{X} = (x_1, x_2, x_3, \dots, x_n)^T$$

f_i — ЦЕЛЕВАЯ ФУНКЦИЯ, $\vec{X}$ — ВЕКТОР РЕШЕНИЙ,
S — НЕПУСТАЯ ОБЛАСТЬ ОПРЕДЕЛЕНИЯ

КРИТЕРИЙ ЭФФЕКТИВНОСТИ (ИСПОЛЬЗОВАНИЕ КРИТЕРИЯ ПАРЕТО)

ДЛЯ ПОЛУЧЕНИЯ ОПТИМАЛЬНЫХ ПО ПАРЕТО РЕШЕНИЙ ПРИМЕНЯЕТСЯ МЕТОД СКАЛЯРИЗАЦИИ ПУТЕМ ВЗВЕШЕННОГО СУММИРОВАНИЯ:

$$F_1\left(\vec{F}(\vec{X})\right) = w_1 f_1(\vec{X}) + \dots + w_r f_r(\vec{X})$$

ПРЕДЛАГАЕМЫЙ СПОСОБ

КОМПОНЕНТЫ ВЕКТОРА $\vec{X}$ - ЗНАЧИМЫЕ БИТЫ TOS:

X_1 — ЗНАЧЕНИЕ ПРИОРИТЕТА (3 БИТА TOS), X_2 — ТРЕБОВАНИЯ К ЗАДЕРЖКЕ,
X_3 — ТРЕБОВАНИЯ К ПРОПУСКНОЙ СПОСОБНОСТИ, X_4 — ТРЕБОВАНИЯ К НАДЕЖНОСТИ

В КАЧЕСТВЕ ЦЕЛЕВЫХ ФУНКЦИЙ ОПРЕДЕЛЕНЫ СЛЕДУЮЩИЕ ФУНКЦИИ:

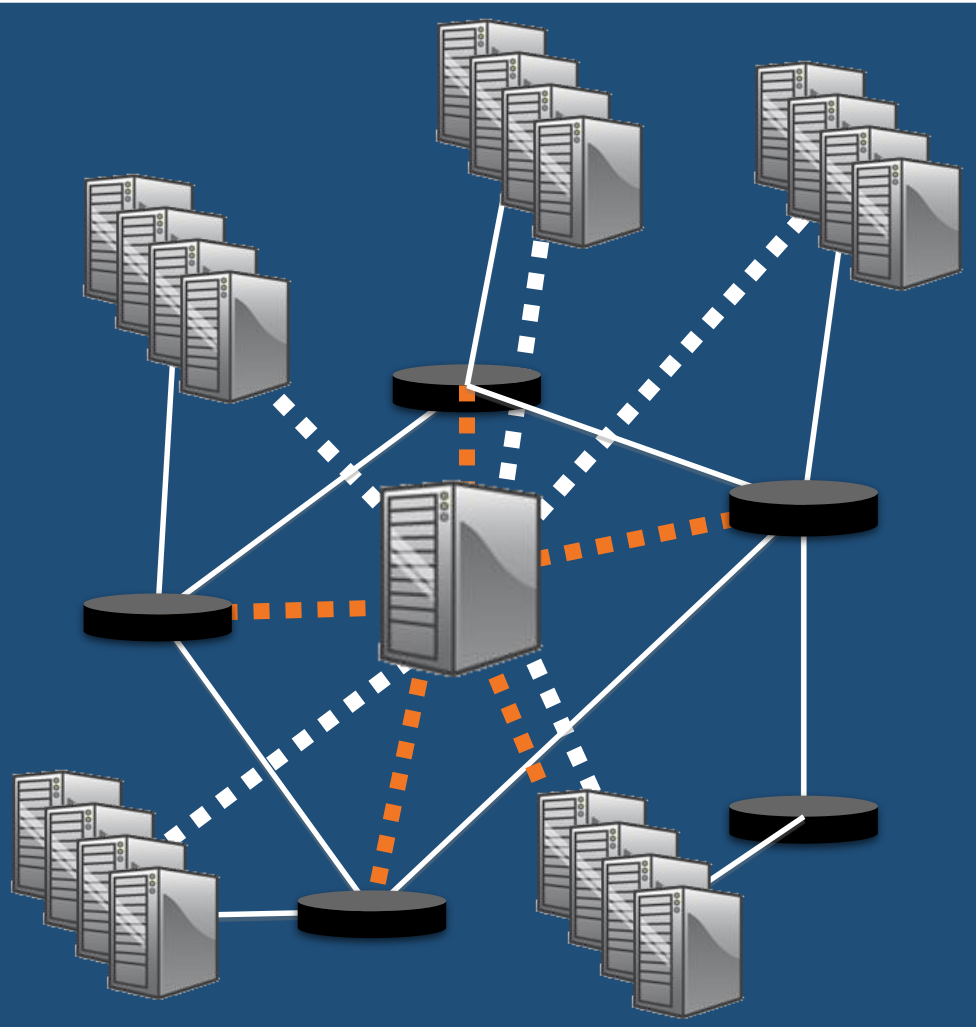
$$f_1(\vec{x}) = \begin{cases} X_1, 0 \le X_1 \le 2 \\ 2X_1, 3 \le X_1 \le 5 \\ 3X_1, 6 \le X_1 \le 7 \end{cases} \qquad f_2(\vec{x}) = X_1 X_2 \qquad f_3(\vec{x}) = X_1 X_3 \qquad f_4(\vec{x}) = X_1 X_4$$

СКАЛЯРИЗАЦИЯ С ПОМОЩЬЮ ВЗВЕШЕННОЙ СУММЫ ПРИ ФОРМИРОВАНИИ ТАБЛИЦ СЕТЕВЫХ ПОТОКОВ ДЛЯ ПКС:

$$F_1\left(\vec{F}(\vec{X})\right) = w_1 f_1(\vec{X}) + w_2 f_2(\vec{X}) + w_3 f_3(\vec{X}) + w_4 f_4(\vec{X})$$

УНИВЕРСАЛЬНОСТЬ МЕТОДА: ДЛЯ КАЖДОЙ СЕТЕВОЙ СИСТЕМЫ МОГУТ БЫТЬ ОПРЕДЕЛЕНЫ ИНДИВИДУАЛЬНЫЕ ЗНАЧЕНИЯ ВЕСОВЫХ КОЭФФИЦИЕНТОВ w_i

ОБЩАЯ АРХИТЕКТУРА ПРЕДЛАГАЕМОЙ СИСТЕМЫ ДЛЯ ПРОГРАММНО-КОНФГУРИРУЕМЫХ СЕТЕЙ



ПОТОК СОБЫТИЙ С РАЗЛИЧНЫХ УРОВНЕЙ ПК

ВЗАИМОДЕЙСТВИЕ С СЕТЕВЫМИ УСТРОЙСТВАМИ

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИС НА КОНТРОЛЛЕРЕ ПКС:

- АНАЛИЗ СОБЫТИЙ, ПОЛУЧЕННЫХ С РАЗЛИЧНЫХ УРОВНЕЙ ПК, ВОССТАНОВЛЕНИЕ ГРАФА, АНАЛИЗ ГРАФА, ПРИНЯТИЕ РЕШЕНИЯ О НЕОБХОДИМОСТИ ОТКЛЮЧЕНИЯ УЗЛА ОТ СЕТИ ИЛИ ПЕРЕСТРОЕНИЯ ТЕКУЩИХ МАРШРУТОВ ПЕРЕДАЧИ ДАННЫХ
- ОЦЕНКА СПОСОБНОСТИ СИСТЕМЫ К ГОМЕОСТАЗУ И ОБЪЕМА ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ, ОПРЕДЕЛЕНИЕ НЕОБХОДИМОСТИ ПЕРЕСТРОЕНИЯ ТЕКУЩИХ МАРШРУТОВ ПЕРЕДАЧИ ДАННЫХ
- УПРАВЛЕНИЕ СЕТЕВЫМ ОБОРУДОВАНИЕМ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА OPENFLOW, РАЗДЕЛЕНИЕ СЕТЕВЫХ УСТРОЙСТВ НА ТЕ, КОТОРЫЕ ПРИНИМАЮТ НА СЕБЯ ДЕСТРУКТИВНЫЕ ВОЗДЕЙСТВИЯ И ТЕ, КОТОРЫЕ ОБЕСПЕЧИВАЮТ НУЖНЫЙ УРОВЕНЬ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ИС

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

1. Проведен анализ современного ВПО и средств защиты, который показал, что для обнаружения современного ВПО необходим комплексный подход к обнаружению нарушений безопасности на всех уровнях ИС
2. Предложен иерархический подход к анализу безопасности ИС, который осуществляет многоуровневый анализ событий, происходящих в ИС
3. Разработана иерархическая графово-событая модель межкомпонентного взаимодействия, определены события, которые необходимо обрабатывать для каждого уровня ИС
4. Предложен подход к управлению безопасностью ИС с использованием оценки способности системы к гомеостазу
5. Проведен анализ технологии ПКС, который показал возможность применения разработанных подходов. Проведены экспериментальные исследования, показавшие эффективность предлагаемого подхода

КАФЕДРА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ»

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

СПАСИБО ЗА ВНИМАНИЕ!