



ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Модернизации объектов информатизации на базе компьютерных сетей в защищенном исполнении

Обоснование необходимости модернизации

1. Потребность в увеличении скорости передачи данных
2. Потребность в увеличении пропускной способности сети
3. Необходимость построения дополнительных маршрутов при передаче данных
4. Необходимость выполнения сертификационных требований, выявленных при аудите сети
5. Модернизация одного элемента сети может вызвать необходимость модернизации связанных с ним элементов инфраструктуры сети

Задачи:

- снижение затрат на обслуживание
- ускорение производительности сетевого оборудования и пропускной способности сети
- замена устаревшего оборудования
- ликвидация периодических или постоянных проблем в работе сети
- получение новых функций администрирования
- Повышение безопасности передачи данных

Обоснование необходимости модернизации

Проблемы программной части:

- нарушения в работе служб DHCP и DNS
- неправильные настройки средств защиты информации
- неверный выбор параметров пользовательских данных
- связанные с протоколом передачи данных (TCP/IP)
- неправильная конфигурация сетевого оборудования

Проблемы аппаратной части:

- помехи внутри сети
- повреждения кабеля
- столкновения пакетов в сети
- некачественный обжим коннекторов
- поломки сетевых карт
- широковещательный шторм, вызванный неправильной настройкой оборудования

Этапы модернизации

Модернизация компьютерной сети происходит в несколько этапов:

Диагностика. Сбор, сравнение и анализ функциональных параметров сети чрезвычайно важны для составления практического обоснования модернизации сети.

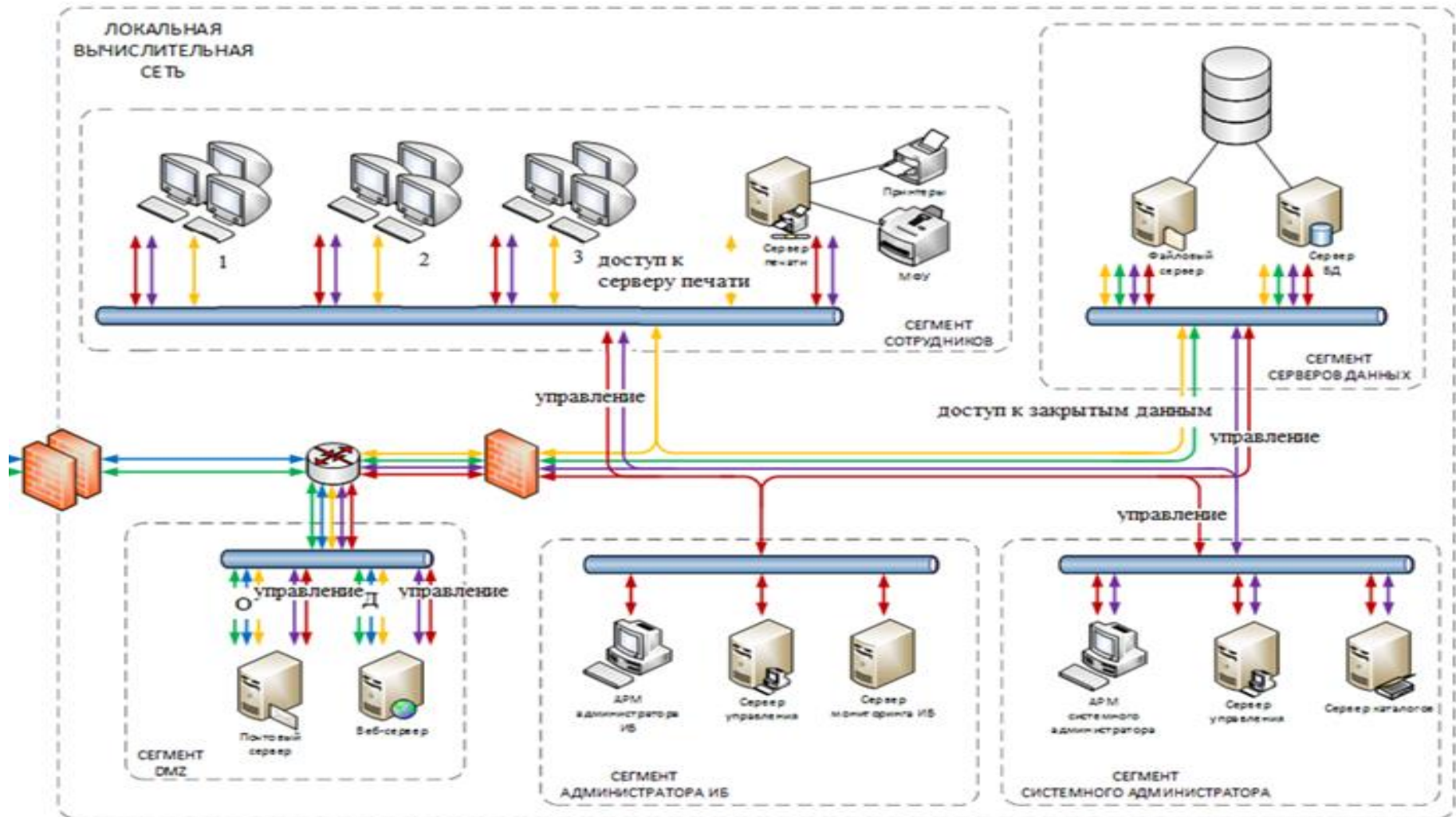
Составление проекта оптимизации с учетом требований защищенности (модели угроз, требований к СЗИ, стоимости). При анализе затрат важно также рассмотреть последствия отказа от предлагаемой модели модернизации или проведения иной модернизации.

Работы по монтажу.

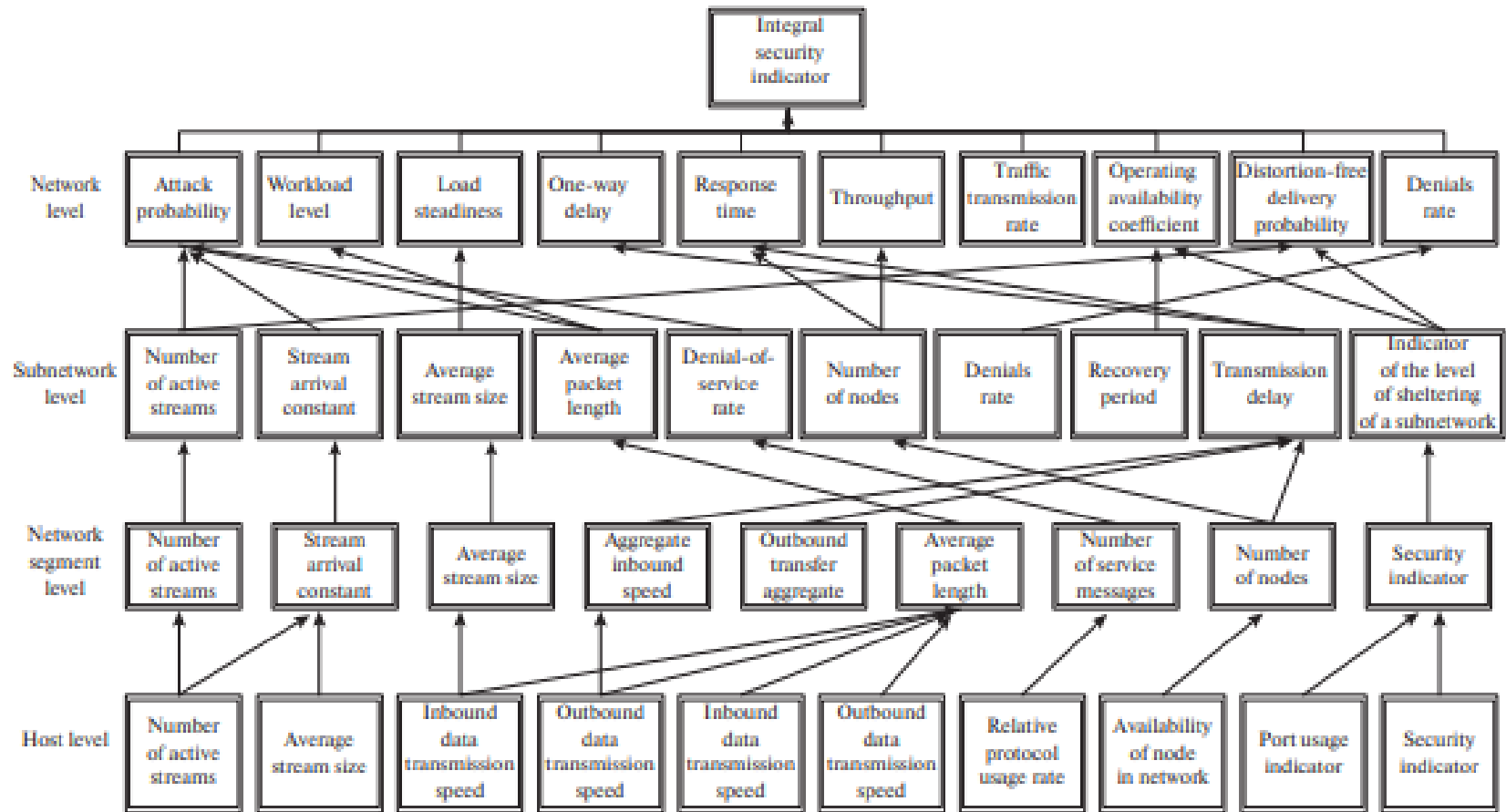
Настройка оборудования.

Аттестация объекта на соответствия категории защищённости

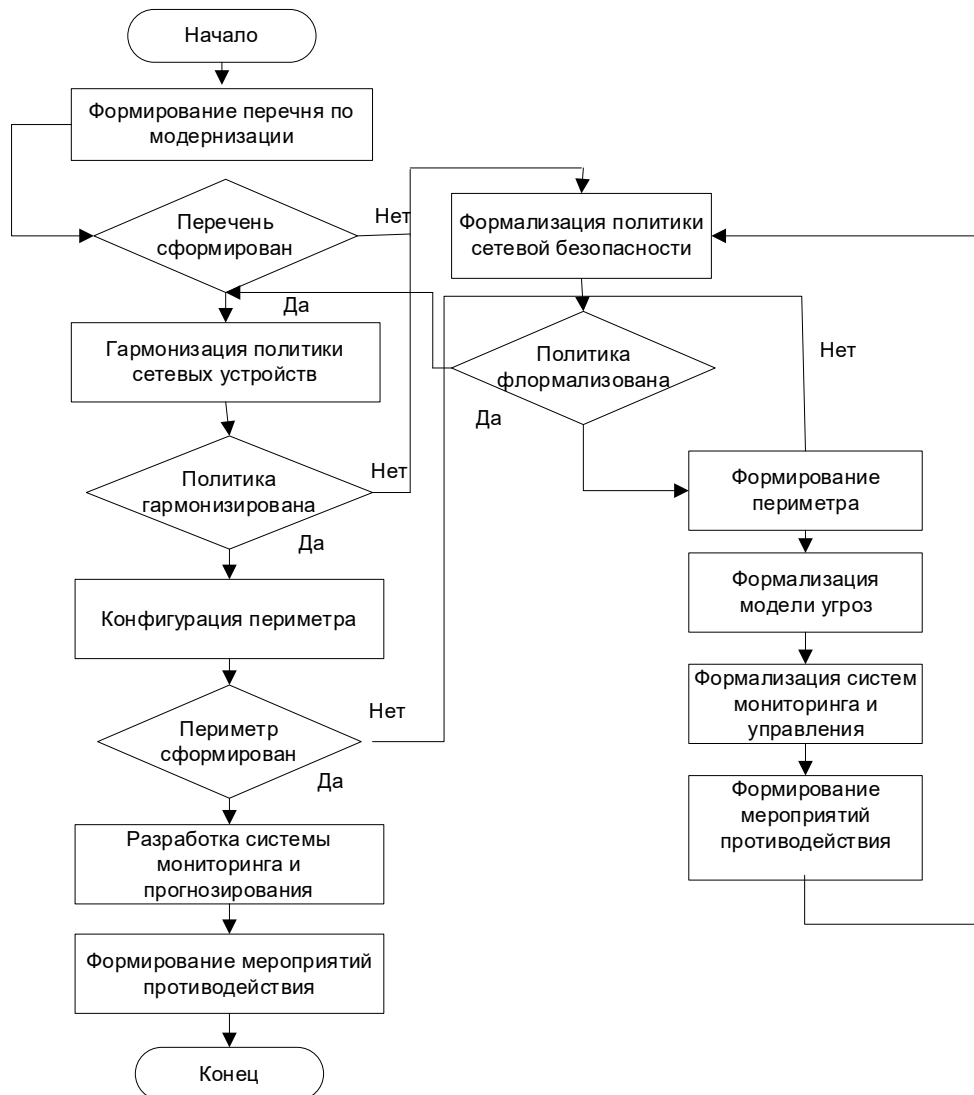
Диагностика



Диагностика



Проект модернизации



Алгоритм формирования периметра

Реконфигурация на базе КЛА

Шаг 1. Декомпозиция множества структурно-функциональных элементов сети S_i с возможностью ранжирования элементов по значимости выполнения целевой функции

Шаг 2. Формируется множество нарушений функционирования сети характеризующего изменения структурных и функциональных характеристик устройств состоящее из подмножества нарушений процессов

$X_{opp}(t, c, y) \rightarrow X_{opp}(t, c, y)' \rightarrow X_{opp}(t, c, y)'' \dots \in X_{Opp'}(t, c, y) \subseteq X_{Opp(1 \dots M)}$ и подмножества показателей нарушения функционирования элементов

Шаг 3. Генерация вариантов множества модернизации сетевой инфраструктуры $G_{рекн}$ структурно-функциональной схемы и процессов передачи:

3.1 Определение вероятностного пространства (C, I, P) нарушений процесс передачи (из шага 2,) где C множеством состояний, соответствующей алгебраической I , и вероятностной меры P .

3.2 Определение подмножества структурных элементов X_{S_i} (из шага 1), которые могут участвовать в перестроении критических важных элементов сети при наступлении состояния C_i , таких, что позволяет осуществить выбор минимум из 2 вариантов структурных элементов с учетом λ — интенсивности отказа элементов, то есть: $S_{i_\lambda} = \{X_{S_i} \in S_{i_\lambda} \mid i = \overline{1, 2}\}$.

3.3. Формирование множества согласующих правил, позволяющих задавать отношения предпочтения $(\varphi^P) \in P$ в условиях протекания элементарных событий.

3.4. Построение множества сценариев реконфигурации $G_{рекн} = [S_{i_\lambda}, \varphi^P, F_{\min}]$ для каждого варианта нарушений процесса передачи.

Шаг 4. Выбор варианта модернизации в соответствии с целью сохранения наиболее приоритетной функции защиты

Реконфигурация на базе РПС

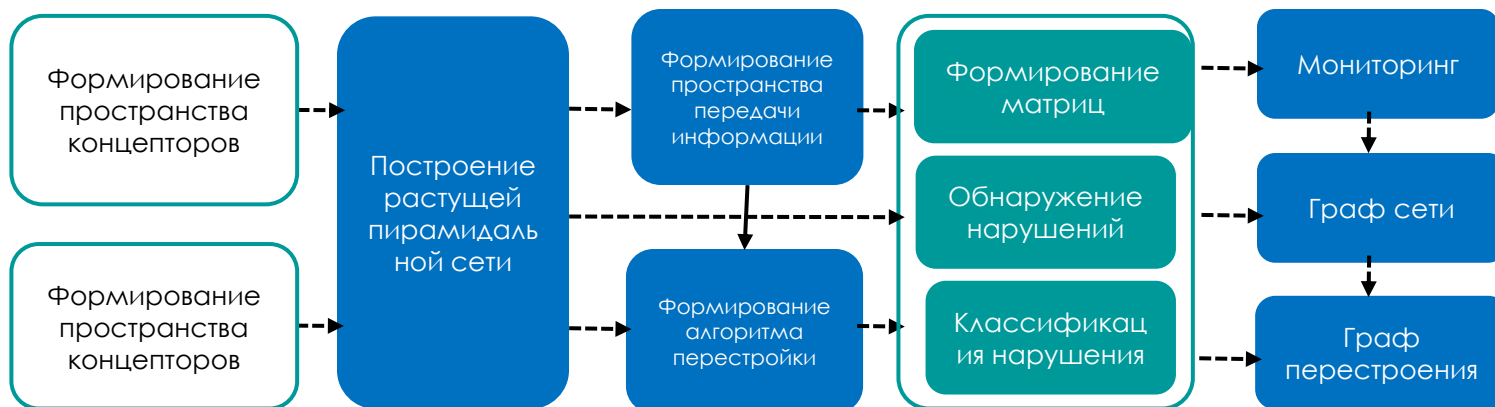
1 Формирование пространства признаков сетевых характеристик

2 Формирование растущей пирамидальной сети

3 Алгоритм реконфигурации сети

4 Выбор альтернативных маршрутов передачи

5 Реконфигурация



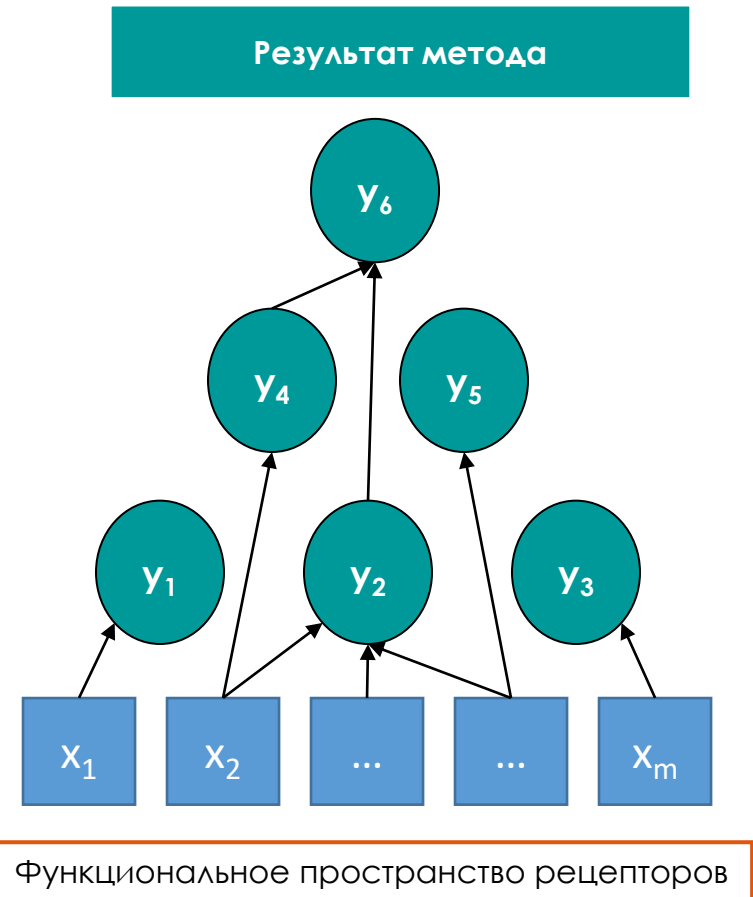
Реконфигурация на базе РПС

Step 1 Установление пространства рецепторов $X=\{x_1, x_2, \dots, x_n, n=1, 2, \dots, m\}$, которое в общем виде можно охарактеризовать как кортеж $x_i=\langle id, type, \Phi, NPr \rangle$,

Step 2 Установление пространства концепторов $Y=\{y_1, y_2, \dots, y_k, n=1, 2, \dots, m\}$,

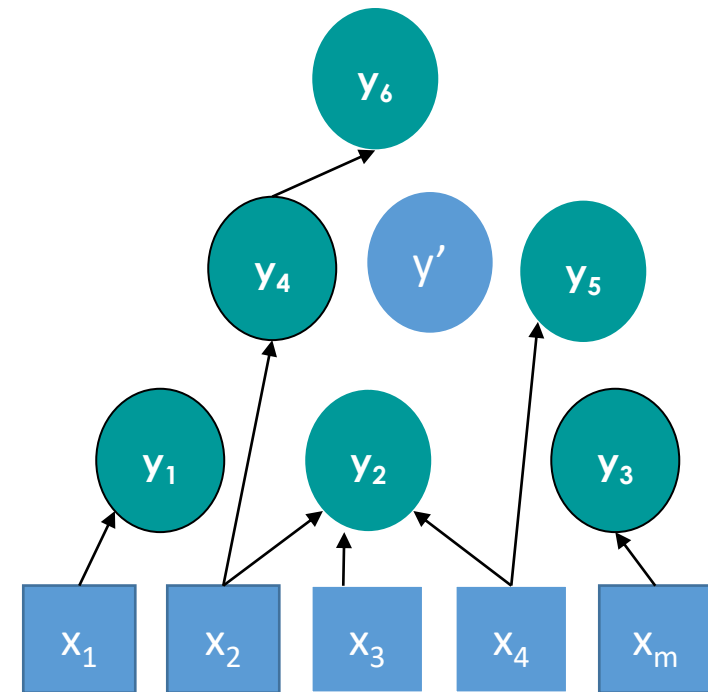
Step 3 Отображение связей графа E путем формирования многоуровневых связей таким образом, чтобы вершины входного слоя были соединены исходящими дугами с вершинами нижележащего слоя, путем сборки сопряженных групп обобщающих и детализирующих объектов.

Step 4 Формирование набора сценариев взаимодействия за счет упорядочения сетевых структур, представленных набором рецепторов



Реконфигурация на базе РПС

- Step 1** Установление нарушений функционирования, за счет изменения характеристик из пространства рецепторов $X=\{x_1, x_2, \dots, x_n, n=1, 2, \dots, m\}$,
- Step 2** Концепция и рецептор, участвующие в процессе перестройки, переводятся в состояние возбуждения, если все вершины маршрута возбуждены, и они сохраняют состояние возбуждения во время всех операций перестройки сети
- Step 3** Генерация вариантов набора перестроек происходит на подмножестве возбужденных концепций и рецепторов.
- 3.1** Устранение дуг, соединяющих возбужденные вершины концепторов/рецепторов.
- 3.2** Введение новой концепции, позволяющей сформировать достижение цели, связанной путем ввода дуг с вершинами многих возбужденных рецепторов.
- 3.3** Подключение к недавно введенной концепции исходящей дуги с не возбужденной родительской вершиной, ведущей к цели и переходу к новой вершине.
- Step 4** Если набор возбужденных сетевых вершин /рецепторов, не имеющих других возбужденных вершин, содержит более одного элемента, к сети присоединяется новый концептор, который подключается путем ввода дуг ко всем вершинам /рецепторам.



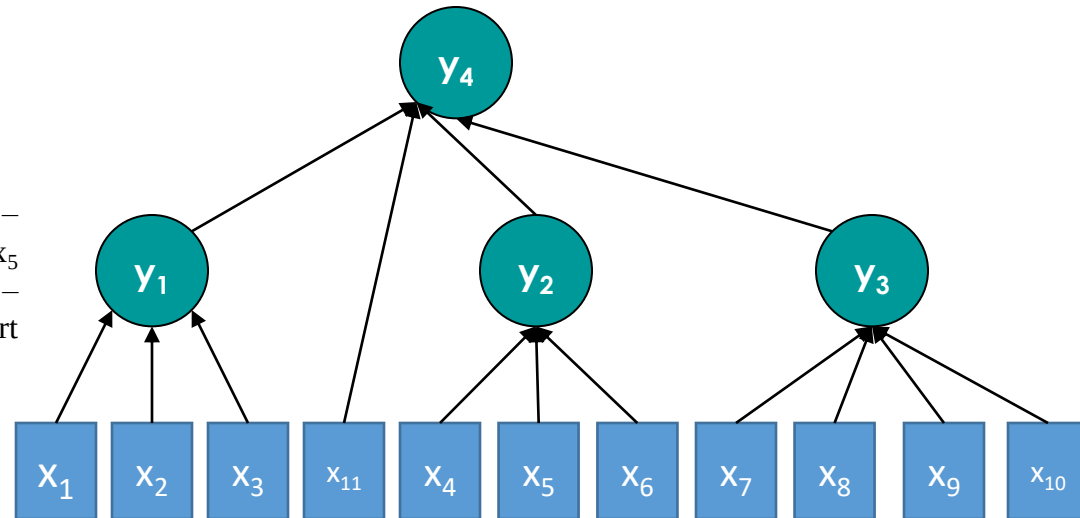
Результат применения метода

Реконфигурация на базе РПС

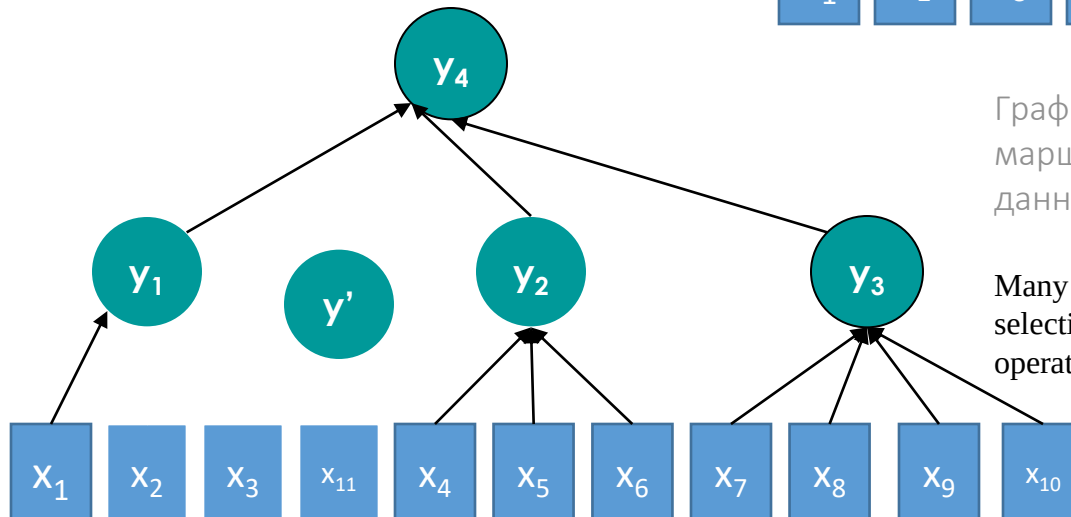
Графическое представление GPN
маршрутизатора в обычном режиме работы

where the set of receptors that includes

x_1 – IP- IP address device; x_2 – routing protocols; x_3 – MAC- address device; x_4 – destination network mask; x_5 – IP-address destination networks; x_6 – route metric; x_7 – protocol type; x_8 – IP- destination address; x_9 – port source; x_{10} – destination port; x_{11} – IP address router.

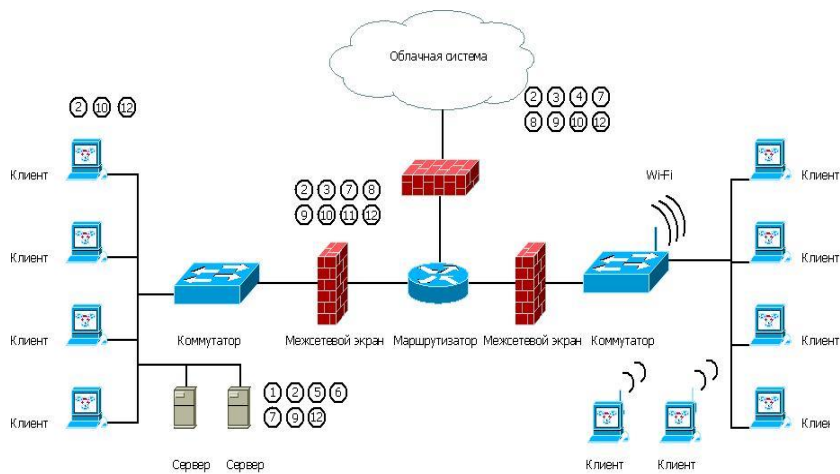


Графическое представление GPN работы
маршрутизатора на примере нарушения передачи
данных

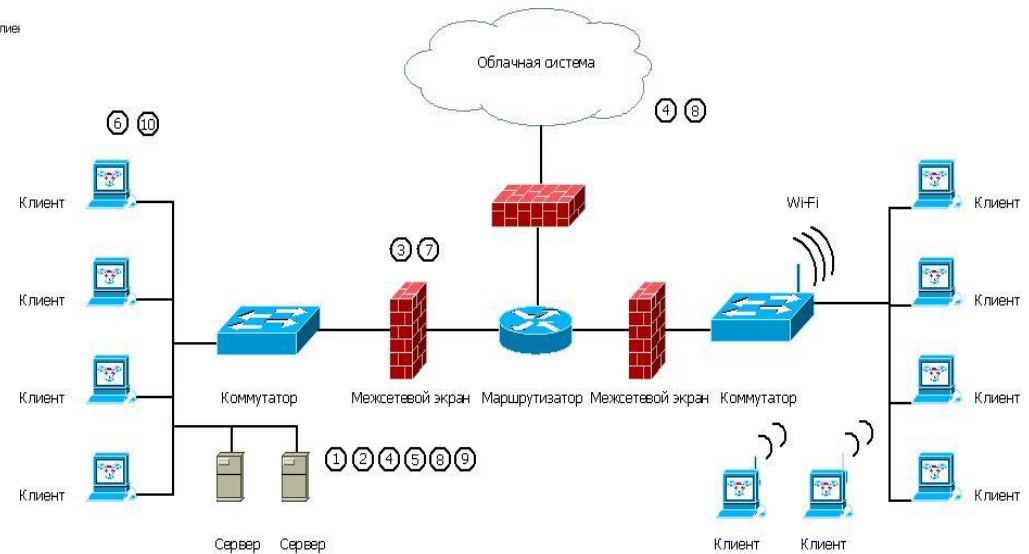


Many concepts that include: y_1 – routing process; y_2 – routing selection; y_3 – rule-based traffic filtering; y_4 – router operation process

Заключение



- | | |
|---|------------------------------------|
| 1 вычисление коэффициентов расстояния и подобию распределений | 7 метод опорных (поворотных) точек |
| 2 модель гауссовских смесей | 8 нейтрализация источника DDoS |
| 3 оценка характеристик входящего потока | 9 расчёт частот TCP-флагов |
| 4 вычисление разности энтропий трафика | 10 вейвлет-анализ сетевого трафика |
| 5 вычисление разности энтропий сессий | 11 фрактальный анализ |
| 6 вычисление разности энтропий с TCP-флагами | 12 прогнозирование трафика |



- | | |
|---|--|
| 1 вычисление коэффициентов расстояния и подобию распределений | 6 вейвлет-анализ сетевого трафика |
| 2 модель гауссовских смесей | 7 фрактальный анализ |
| 3 оценка характеристик входящего потока | 8 прогнозирование трафика |
| 4 расчёт энтропии | 9 анализ сингулярного спектра |
| 5 расчёт частотных характеристик пакетов | 10 анализ векторных потоков информации |

Литература

1. Приказ ФСТЭК от 29 апреля 2021 г. № 77. Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.
2. Бусленко Н. П. Моделирование сложных систем. - 2-е изд., перераб. - Москва : Наука, 1978. - 399 с. : ил.; 22 см.
3. Фаткиева Р.Р., Шичкина Ю.А. Метод реконфигурации промышленных объектов с применением аппарата кусочно-линейных агрегатов // Вестник машиностроения. 2021. № 6. С. 40-46.
4. Гладун В.П. Партнерство с компьютером. Человеко-машинные целеустремленные системы. — Киев: Port-Royal, 2000. — 118 с
5. Shichkina, Y. A., Fatkueva R. R. Detection of network attacks using of growing pyramid networks // 2021 10th Mediterranean Conference on Embedded Computing, MECO 2021: 10, Budva, 07-10 июня 2021 года. - Budva, 2021. - P. 9460188. - DOI 10.1109/MECO52532.2021.9460188