СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Модернизации объектов информатизации

СПбГЭТУ «ЛЭТИ», 2021 г.

9. МОДЕРНИЗАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

9.1 Обоснование необходимости модернизации

При проектировании ЛВС изначально целесообразно закладывать в характеристики сети возможность ее масштабировать и оптимизировать для повышения эффективность всей системы. Модернизации ЛВС предполагает улучшение ее работы. Для этого на первом этапе необходимо проанализировать:

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. Масштабируемость сетевой инфраструктуры, поскольку модернизация одного элемента сети может вызвать необходимость реконфигурацию связанных с ним элементов инфраструктуры сети.

Если на этапе обследования выявлены перечисленные проблемы необходимо отдельно оценить проблемы аппаратной и программной частей функционирования ЛВС, в частности:

-проблемы программной части:

- нарушение в работе сетевых служб (DHCP,DNS, ICMP);
- неправильные настройки средств защиты информации;
- неверный выбор параметров пользовательских данных;
- нарушения, связанные с неправильной настройкой стека TCP/IP;
- неправильная конфигурация сетевого оборудования;

проблемы аппаратной части:

- помехи внутри сети;
- повреждения кабеля;
- коллизии в сети;
- некачественный обжим коннекторов;
- поломки оборудования и сетевых карт;
- широковещательный шторм, вызванный неправильной настройкой оборудования.

При оценивании аппаратной части необходимо обратить внимание на оборудование, которое функционирует достаточно долгое время, в частности работу пограничных шлюзов между ЛВС. Поскольку в ряде случаев будет целесообразно осуществлять замену оборудования, а не осуществлять его модернизацию. При этом необходимо оценить стоимость каждого из решений и его влияние на поддерживаемые сервисы, это позволить определить, какая из стратегий лучше- модернизация или полная замена оборудования.

Оценивание программного обеспечения связано с необходимостью преобразования форматов, контролем доступа или оценкой расстояния между конечными точками. При этом функция защиты и преобразование форматов может предполагать аппаратную реализацию, тогда стоимость модернизации необходимо обосновать для анализа экономических выгод. Одним из популярных и сравнительно простых методов является анализ затрат, при котором общая стоимость модернизации сравнивается с ожидаемыми выгодами. В этом случае к задачам модернизации сетевой инфраструктуры можно отнести:

- снижение затрат на обслуживание;
- ускорение производительности сетевого оборудования и пропускной способности сети;
- замену устаревшего оборудования;
- ликвидацию периодических или постоянных проблем в работе сети;
- получение новых функций администрирования;
- повышение безопасности при передаче данных.

Если стоимость модернизации приемлема, то возможно приступать к этапу реализации проекта. При анализе затрат важно также рассмотреть последствия отказа от предлагаемого варианта модернизацию. Это необходимо учитывать, поскольку иногда проблему эффективности функционирования сетевой инфраструктуры возможно решить не за счет модернизации, а используя методы реконфигурации сетевого оборудования или потоков данных.

Основная формула расчета эффективности выглядит как:

Отдача от инвестиций = (связанная экономия на эксплуатационных расходах + увеличение доходов за счет сервисов) — (начальные расходы на модернизацию + финансовые издержки + эксплуатационные расходы за данный период).

9.2 Этапы модернизации сетевой инфраструктуры

Модернизация компьютерной сети происходит в несколько этапов:

1. Диагностика. На этом этапе осуществляется сбор, сравнение и анализ функциональных параметров сети и программного обеспечения. Мониторинг работы сетевого оборудования и каналов передачи данных позволяет рассчитать текущую сетевую загрузку и оценить необходимые характеристики сети после модернизации (как трафик между коммутаторами, загруженность каналов, утилизация портов или каналов на коммутаторах или маршрутизаторах, логические потоки данных, общая нагрузка на сеть, долю ошибок при передаче, уровень загруженности сервера). В качестве примера можно привести систему показателей функционирования сети на Рис. 9.1. Прохождение этого этапа позволяет выявить узкие места требующие изменения.

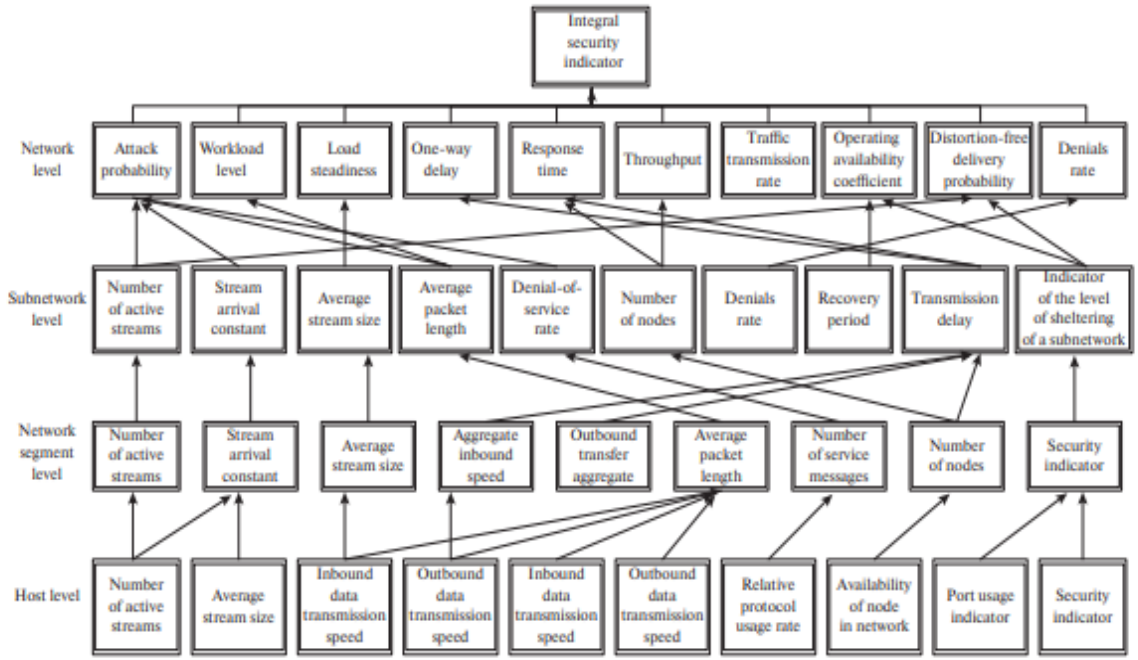


Рис. 9.1

2. Составление проекта оптимизации. На данном этапе необходимо оценить требования к элементам замены, и оценить стоимость модернизации. Однако в частном случае, может возникнуть ситуация,

отсутствия ресурсов на модернизацию. В этом случае целесообразно рассмотреть вопрос о реконфигурации сетевой инфраструктуры. *Реконфигурация* это– изменение состава и способа взаимодействия программных и аппаратных средств сети с целью изменения ее устоявшейся топологии передачи данных. В обоих случае при составлении проекта необходимо учитывать требования защищенности (вносить изменения в модель угроз, требований к СЗИ, политику безопасности и др). Внесение изменений в сетевую инфраструктуру требует внесение дополнительных изменений в периметр мониторинга и контур управления средства защиты информации, с включением в него множества структурных элементов для оценки их функционирования в процессе функционирования. Это позволяет достигнуть необходимый уровень функционирования, а также системное согласование всех используемых мер, методов и средств управления (Рис. 9.2).

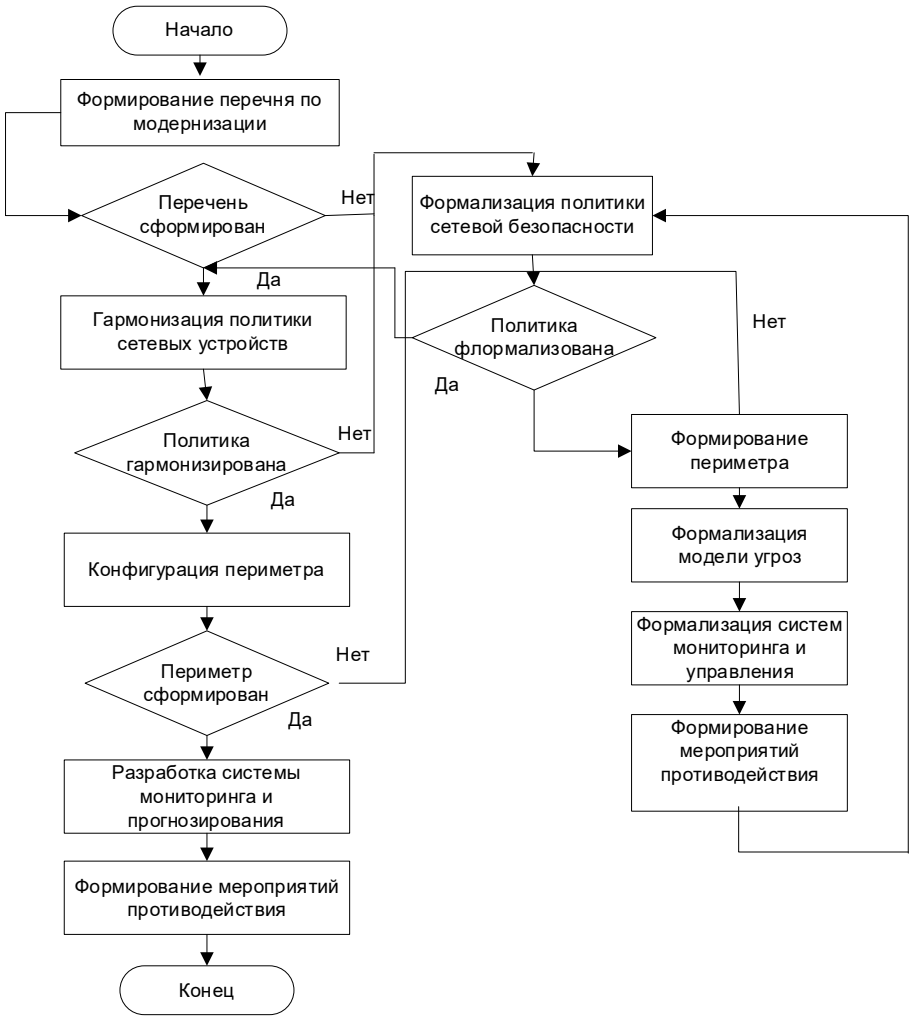


Рис. 9.2

3. Работы по монтажу.
4. Настройка оборудования.
5. Аттестация объекта на соответствия категории защищённости и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний) [1], в результате которых подтверждается соответствие объекта требованиям по защите информации в условиях его эксплуатации. Допускается проведение аттестации объекта на этапе его эксплуатации в случае, если владельцем объекта принято решение об обработке защищаемой информации после ввода в эксплуатацию объекта.

9.3 Реконфигурация с использованием аппарата кусочно-линейных агрегатов

Рассмотрим метод реконфигурации сетевой инфраструктуры с использованием аппарата кусочно-линейных агрегатов [1, 2]. Метод состоит из следующих шагов:

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, характеризующее изменения структурных и функциональных характеристик устройств состоящее из подмножества нарушений процессов и подмножества показателей нарушения функционирования элементов

Шаг 3. Генерация вариантов множества модернизации сетевой инфраструктуры $G_{\text{рекн}}$ 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 $\lambda -$ интенсивности отказа элементов, то есть:$S_{i_\lambda} = \{X_{S_i} \in S_{i_\lambda} \quad | i = \overline{1,2}\}$.

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

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

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

Применение метода целесообразно при замене отдельных сетевых устройств или подсистем (например реконфигурация интерфейсов сетевых устройств или перестроении критических важных элементов).

9.4 Реконфигурация на базе использования аппарата растущих пирамидальных сетей

Растущей пирамидальной сетью (РПС) называется ациклический ориентированный граф, в котором нет вершин, имеющих одну заходящую дугу [4]. Вершины, не имеющие заходящих дуг, называются рецепторами, остальные вершины – концепторами. В обобщённом виде РПС является многоуровневой структурой, где каждый уровень является объединением признакового пространства предыдущего уровня сетевой структуры. В отличие от нейроподобных сетей в РПС эффект обнаружения атак достигается без введения априорной избыточности сети.

В начальном состоянии сеть состоит только из рецепторов. Концепторы формируются в результате работы алгоритма построения сети. Алгоритм, описанный в ряде публикаций [4,5], предназначен для работы в ситуациях, когда признаковое описание каждого объекта сети полностью известно и вводится целиком. При появлении новых признаков, характеризующих объект, необходимо формировать новое полное описание объекта, и заменять представляющую его пирамиду другой, соответствующей новому описанию.

Рассмотрим модель РПС компьютерной сети, представляющую собой сетевую структуру, в виде ациклического графа:

$$G(V, E), \qquad (1)$$

содержащего уровни вершин V и E – множество связей между вершинами. При этом нижний уровень вершины графа $V(X)$ формируется за счет установления связей вершины и признакового пространства рецепторов $X =$

$\{x_1, x_2 \dots, x_n, n = 1, 2, \dots, m\}$, которые в общем виде можно характеризовать кортежем:

$$x_i = < \mathrm{id}, \mathrm{type}, \Phi, \mathrm{NPr} >, \qquad (2)$$

где id идентификатор элемента сетевой инфраструктуры; type - тип элемента сетевой инфраструктуры; $\Phi_{x_i} = \{\varphi^{m}_{x_{i_1}}, \varphi^{m}_{x_{i_2}}, \dots, \varphi^{m}_{x_{i_k}}\}$ - множество функций, реализуемых вершиной x_i, где верхний индекс $m \epsilon \{0; 1\}$ обозначает режим выполнения функции (использует ли компонент x_i функциональность $\varphi_{x_{i_j}}$ в текущем процессе или нет); NPr - число процессов, в которых задействован данный элемент сетевой инфраструктуры. Второй и последующие уровень вершин графа формируется за счет множества вершин-концепторов, представленных вершинами нижестоящего уровня графа.

Все потоки информации, циркулирующей между компонентами РПС формируют множество дуг графа $E = \{e_1, \dots, e_n, n = 1, 2, \dots, k\}$, где e_i - элементы множества дуг, n - количество дуг графа. Исходящая из вершины дуга означает, что данная вершина осуществляет управляющее информационное воздействие на другую вершину. Отображение дуг задает структуру многоуровневых связей так, что вершины первого уровня связаны исходящими дугами с вершинами последующих уровней, образуя соответственно конъюнктивные группы обобщающих и детализирующих признаков. Таким образом, модель РПС является сетевой моделью, в структуре которой объединены образы всех сценариев взаимодействия элементов и систем, составляющих сетевую структуру компьютерной сети.

Важнейшим преимуществом РПС является возможность перестроения ее функционирования за счет изменения связей между ее элементами. Это позволяет построить структурную схему функционирования компьютерной сети в условиях множества различных маршрутов передачи информации (дуг) и выявить изменения характеристик ее элементов (концепторов). Сравнение РПС, в режиме штатного функционирования с РПС с изменёнными характеристиками позволяет идентифицировать структурные нарушения безопасности. Рассмотрим шаги метода обнаружение атаки, с использование аппарата РПС (Рис.9.3):

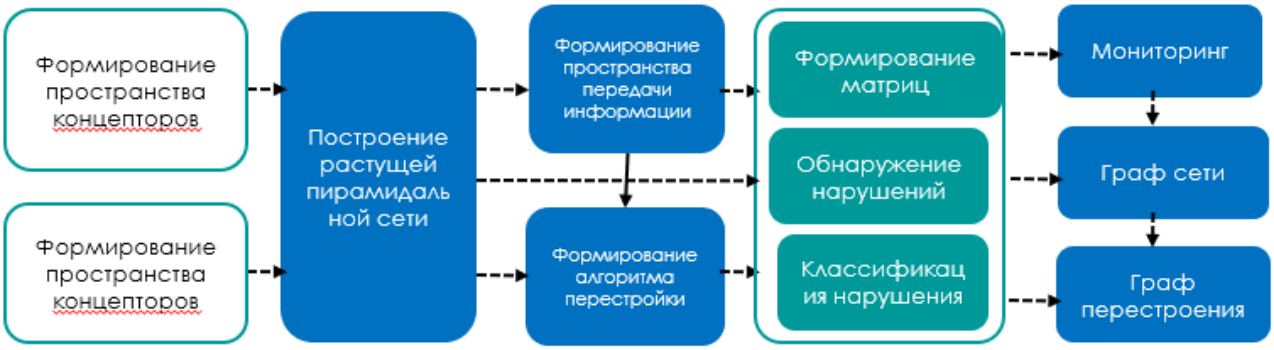
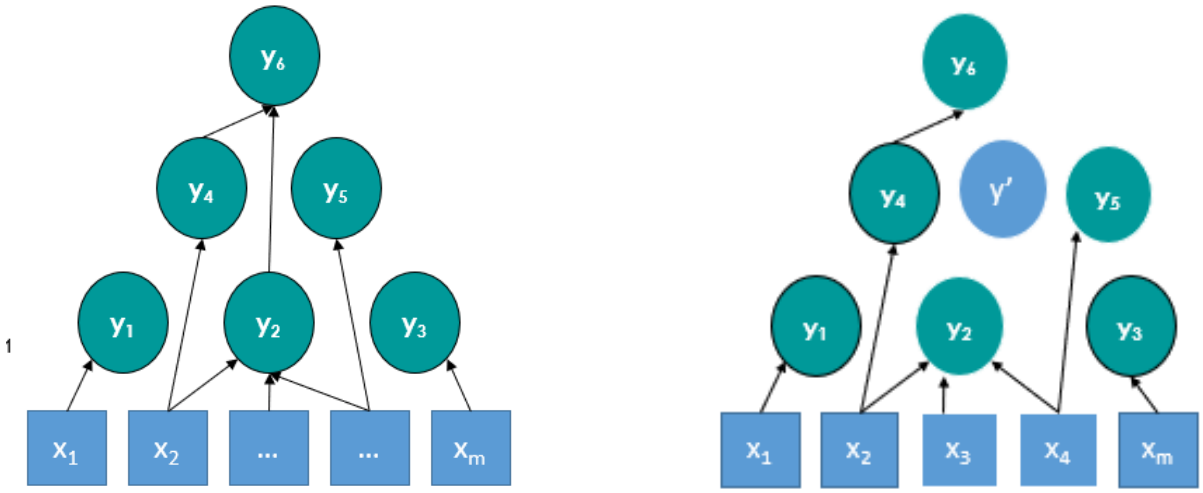


Рис. 9.3

1. Установление пространства рецепторов $X=\{x_1,x_2...,\ x_n,\ n=1,2,...,m\}$, которое в общем виде можно охарактеризовать как кортеж x_i=<id, type, Ф, NPr>,
2. Установление пространства концепторов $Y=\{y_1,y_2,...,\ y_k,\ n=1,2,...,m\}$,
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.
4. Формирование набора сценариев взаимодействия за счет упорядочения сетевых структур, представленных набором рецепторов (Рис 9.4 а). В результате работы этого шага получаем графическую схему функционирования РПС компьютерной сети в штатном режиме функционирования.
5. Выявление изменений значений рецепторов $X=\{x_1,x_2...,\ x_n,\ n=1,2,...,m\}$ с поиском концептора, участвующего в маршруте сетевой передачи.



а) б)

Рис.9.4

6. Вывод концептора из маршрута передачи информации.
7. Поиск концептора, способного взять на себя функции, исключенного на шаге 6 концептора. В противном случае формирование нового концептора (Рис 9.4.б).
8. Перестроение маршрута передачи данных с учетом концептора, сформованного на шаге 7.

Преимущество представленных подходов отличаются возможностью учета структурной топологии компьютерной сети, ее функциональных особенностей, а также маршрутов передачи информации. Поиск и обнаружение нарушений передачи данных производится на основании рассмотрения множества характеристик объектов и процессов, позволяющих ввести дополнительные связи на множестве элементов сетевой инфраструктуры, и приводящее к обнаружению изменения сетевой структуры при ее функционировании.

СПИСОК ЛИТЕРАТУРЫ

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., Fatkieva 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