# Разработка математической модели универсальной ЛВС с учётом требований информационной безопасности

Оглавление

[Разработка математической модели универсальной ЛВС с учётом требований информационной безопасности 0](#__RefHeading__926_2137358750)

[1. Введение. 1](#__RefHeading__928_2137358750)

[3. Состав модели. 2](#__RefHeading__930_2137358750)

[3.1. Представления. 2](#__RefHeading__932_2137358750)

[3.1.1. Общее представление. 3](#__RefHeading__934_2137358750)

[3.1.2. Канальное представление. 4](#__RefHeading__936_2137358750)

[3.1.3. Сетевое представление. 5](#__RefHeading__938_2137358750)

[3.2. Целевые функции. 5](#__RefHeading__940_2137358750)

[4. Абстрактная методология модели. 7](#__RefHeading__942_2137358750)

[4.1. Количественная оценка недоступности/конфиденциальности. 7](#__RefHeading__944_2137358750)

[4.2. Агрегирование количественных оценок. 7](#__RefHeading__946_2137358750)

[4.3. Введение нормы в пространстве количественных оценок. 7](#__RefHeading__948_2137358750)

[5. Реализация абстрактных методов модели. 8](#__RefHeading__950_2137358750)

[5.1. Недоступность в канальном представлении. 8](#__RefHeading__952_2137358750)

[5.1.1. Определение. 8](#__RefHeading__954_2137358750)

[5.1.2. Алгоритм агрегирования. 8](#__RefHeading__956_2137358750)

[5.1.3. Примеры вычисления. 8](#__RefHeading__958_2137358750)

[5.1.4. Введение нормы. 8](#__RefHeading__960_2137358750)

[5.2. Недоступность в сетевом представлении. 8](#__RefHeading__962_2137358750)

[5.2.1. Определение. 8](#__RefHeading__964_2137358750)

[5.2.2. Алгоритм агрегирования. 8](#__RefHeading__966_2137358750)

[5.2.3. Примеры вычисления. 9](#__RefHeading__968_2137358750)

[5.2.4. Введение нормы. 9](#__RefHeading__970_2137358750)

[5.3. Конфиденциальность в сетевом представлении. 9](#__RefHeading__972_2137358750)

[5.3.1. Определение. 9](#__RefHeading__974_2137358750)

[5.3.2. Алгоритм агрегирования. 9](#__RefHeading__976_2137358750)

[5.3.3. Примеры вычисления. 10](#__RefHeading__978_2137358750)

[5.3.4. Введение нормы. 10](#__RefHeading__980_2137358750)

[6. Методология построения реальной сети как продукта модели. 11](#__RefHeading__982_2137358750)

[6. Заключение. 12](#__RefHeading__984_2137358750)

# 1. Введение.

Сегодня вопросам информационной безопасности в локальных сетях предприятий уделяется всё большее внимание. Однако, локальные сети - это очень сложные, многоуровневые совокупности устройств, уязвимость какого-либо узла в которых ставит под сомнение безопасность всей сети в целом. Именно поэтому важно взять под контроль надежность, доступность и безопасность сети еще на этапе ее проектирования, учитывая при этом возможные варианты сетей, их совокупности и особенности, взаимное влияние элементов сети друг на друга.

Для решения данной задачи предлагается описать типовую универсальную схему, на основе которой, путем ее оптимизации, возможно построить любую гетерогенную ЛВС, описать математическую модель, а также - произвести качественный и количественный анализ ее устойчивости к угрозам различного вида.

# 2. Обзор литературы.

К сожалению, не было найдено литературы, содержащей количественное описание таких аспектов информационной безопасности как целостность (integrity) и конфиденциальность (confidentiality).

# 3. Состав модели.

Для дальнейших выкладок будем пользоваться так называемыми квазиподсетями - набором конечных узлов и вложенных квазиподсетей, подключенных параллельно к единственной общей точке входа.

Сначала обсудим способ описания квазиподсетей, а затем поговорим о заданных на них целевых функциях, к оптимизации которых и сведётся наша задача проектирования реальной сети.

## 3.1. Представления.

Термин “представление” в рамках нашей модели обозначает способ описания топологии квазиподсети (в том числе и корневой квазиподсети - проектируемой системы). В нашей модели задействованы три уровня модели OSI: физический, канальный и сетевой, - в связи с чем мы выделяем три представления: общее (учитывает топологию квазиподсети как на канальном и физическом уровнях, так и на сетевом уровне модели OSI), канальное (учёт топологии квазиподсети только на канальном уровне модели OSI (а также на физическом уровне, являющемся его компонентом)) и сетевое (учёт только топологии квазиподсети на сетевом уровне). Канальное и сетевое представления строятся на основе общего представления путём упрощения нюансов, не относящихся к задействованным уровням модели OSI.

Все представления в нашей модели являются рекурсивными графами коммуникации, узлами которого являются конечные узлы (ПК, сервера, узлы IP-телефонии, устройства печати и сканирования итд.) и разветвители, к которым подсоединены вложенные графы коммуникации того же рода (каждый граф отвечает квазиподсети той или иной степени вложенности).

### 3.1.1. Общее представление.

Общее представление квазиподсети объединяет в себе описание топологии квазиподсети на всех уровнях в модели OSI с физического по сетевой.

Общее представление корневой квазиподсети строится на основе полного набора входных данных, введённых от пользователя (сведения о физической топологии системы (например, количество офисов, тип связи внутри офиса, тип связи между офисами итд.), сведения о логической топологии системы (например, количество групп пользователей, распределение групп пользователей по офисам итд.)). Группы пользователей распределяются по офисам при помощи технологии VLAN.

При построении общего представления руководствуются следующими принципами:  
1. Коммутатор с настроенными вланами в каждом офисе.

2. Офисы объединяются при помощи маршрутизаторов.

3. На входе в систему располагается сетевой экран.

(Мы разбиваем сетевые экраны на две сущности: глобальный сетевой экран, который определяет разрешённые маршруты внутри системы и который может быть вынесен на вход системы, и встроенные сетевые экраны, которые занимаются определением и фильтрацией “мусорного” трафика. При этом в данной версии модели глобальный сетевой экран определяет правила коммутации только между подсетями, наличие портов внутри подсетей игнорируется.)

### 3.1.2. Канальное представление.

В канальном представлении отражена физическая топология квазиподсети. Разветвителями являются любые физические устройства (маршрутизаторы, коммутаторы), осуществляющие развилку в сети.

Построение канального представления происходит посредством превращения всех устройств, осуществляющих развилку, в разветвители, и игнорирования наличия вланов.

### 3.1.3. Сетевое представление.

В сетевом представлении отражена сетевая топология квазиподсети. Разветвителями являются порты маршрутизаторов, порождающие подсети и/или вланы.

Построение сетевого представления происходит посредством игнорирования наличия коммутаторов, а также объединения фрагментов каждого влана в один, руководствуясь следующим принципом: для каждого влана V удалить все фрагменты V из всех подсетей, объединить в один и подключить в качестве дочерней подсети к маршрутизатору R наинизшего уровня иерархии, в дочерних сетях которого содержится хотя бы один фрагмент влана V, а в дочерних сетях всех маршрутизаторов более высоких уровней иерархии нет ни одного фрагмента V, не принадлежащего дочерним сетям R.

## 3.2. Целевые функции.

Когда говорят о безопасности сети, имеют ввиду два аспекта:

* Целостность (безопасность структуры квазиподсети). Ввиду того, что мы отдельно рассматриваем функционирование квазиподсети на физическом и канальном уровнях и на сетевом уровне, мы будем говорить о целостности в канальном представлении и о целостности в сетевом представлении. В канальном представлении целостность означает устойчивость квазиподсети к нарушениям структуры на физическом (обрыв кабеля) и на канальном (нетаргетированная DDOS-атака) уровнях. В сетевом представлении целостность означает устойчивость квазиподсети к таргетированным DDOS-атакам; при рассмотрении этого типа атак учитывается наличие сетевого экрана на входе в корневую квазиподсеть.
* Конфиденциальность (безопасность данных в квазиподсети). Исключая тривиальные случаи, в которых система заведомо полностью скомпрометирована (когда у злоумышленника есть возможность прийти и унести с собой сервер вместе со всеми хранящимися на нём данными либо когда критичные данные располагаются в одной подсети (в пределах одного офиса)), конфиденциальность описывает свойства квазиподсети, проявляющиеся исключительно на сетевом уровне: сложность получения несанкционированного доступа на чтение и/или запись к критичным данным.

Выберем целевые функции так, чтобы они обладали аддитивностью (недоступность – величина, противоположная целостности):

* недоступность в канальном представлении;
* недоступность в сетевом представлении;
* конфиденциальность в сетевом представлении.

Оговорим здесь основные составные части постановки задачи оптимизации, решаемой в ходе данной работы.

Метод решения задачи оптимизации - применение генетического алгоритма. Обсуждение выбора алгоритмов селекции, скрещивания и мутации находится за пределами настоящей работы.

# 4. Абстрактная методология модели.

## 4.1. Количественная оценка недоступности/конфиденциальности.

При разработке методологии количественной оценки нарушений/компрометации квазиподсети мы сталкиваемся с тем, что эти характеристики проявляются не в статике, а в динамике, причём зависящие от них процессы (разрушения/взлома) могут протекать по-разному в силу различной природы. Поэтому наши количественные оценки должны фиксировать динамику, а не статику системы. Например, в качестве оценки мы можем взять не скаляр, а, например, функцию зависимости некоторой характеристики системы от времени (с начала взлома/разрушения или от настоящего момента).

## 4.2. Агрегирование количественных оценок.

После того, как мы установим вид целевых функций для конечных узлов, нам нужно будет научиться считать их для квазиподсети по значению тех же целевых функции для конечных узлов и вложенных квазиподсетей.

## 4.3. Введение нормы в пространстве количественных оценок.

Для того, чтобы можно было применять генетические алгоритмы, нужно задать (скалярную) фитнес-функцию, которая позволяла бы определить относительную “хорошесть” решения. Введённые в пункте 4.1. оценки могут представляют из себя элементы функционального, а не скалярного, пространства. В этом случае перед применением модели на практике необходимо задать норму в пространстве количественных оценок.

# 5. Реализация абстрактных методов модели.

## 5.1. Недоступность в канальном представлении.

### 5.1.1. Определение.

Недоступность в канальном представлении (НКП) - функция зависимости степени нарушения структуры конечного узла или квазиподсети от времени (0 - ненарушенная структура; 1 - абсолютно нарушенная структура, конечный узел или квазиподсеть полностью неработоспособны).

### 5.1.2. Алгоритм агрегирования.

При агрегировании квазиподсети совокупная НКП рассчитывается через НКП конечных узлов, вложенных квазиподсетей и связей, ведущих к ним, по следующей формуле: , где - узлы и вложенные квазиподсети квазиподсети G,- устройство в точке входа в G, а- соединения междуи.

### 5.1.3. Примеры вычисления.

В простейшем случае НКП узла или соединения можно задать следующей формулой (скорость выхода из строя узла пропорциональна степени выхода его из строя):, где – амортизация (скорость выхода устройства из строя), - наработка на отказ (гарантированная производителем продолжительность работы устройства).

### 5.1.4. Введение нормы.

Естественная норма для оценки НКП - значение НКП в определённый момент времени (например, задаваемый пользователем при помощи ползунка).

## 5.2. Недоступность в сетевом представлении.

### 5.2.1. Определение.

Недоступность в сетевом представлении (НСП) - функция зависимости степени “проседания” узла или связи (отношения скорости передачи данных к скорости передачи в штатном режиме) от времени и интенсивности таргетированной атаки.

### 5.2.2. Алгоритм агрегирования.

При агрегировании квазиподсети совокупная НСП рассчитывается через НСП конечных узлов, вложенных квазиподсетей и связей, ведущих к ним, по следующей формуле:, где - узлы и вложенные квазиподсети квазиподсети G,- устройство в точке входа в G.

### 5.2.3. Примеры вычисления.

В простейшем общем случае НСП узла можно задать формулой, где- объём оперативной памяти маршрутизатора,- интенсивность атаки (в еденицах гигабайт/сек.). В случае модификаций зависимость будет более сложной. Например, при добавлении интеллектуальной системы распознавания мусорного трафика НСП может быть описана формулой, где- пороговый объём отсекаемого “мусорного” трафика.

### 5.2.4. Введение нормы.

Пользователю предлагается на выбор одна из двух естественных норм:

1. максимальное “проседание” за бесконечное время при заданной пользователем эталонной интенсивности атак;
2. время, требуемое, чтобы узел полностью “лёг” при заданной пользователем эталонной интенсивности атак.

## 5.3. Конфиденциальность в сетевом представлении.

Для дальнейших рассуждений требуются знание об открытости или закрытости (то есть, о наличии прямого доступа к интернету) узлов на основе начальных данных от пользователя. Из закрытых узлов выбирается (в качестве одной из переменных в задаче оптимизации) сервер - целевой узел, содержащий критические данные. Будем считать взломом несанкционированный доступ к серверу извне.

### 5.3.1. Определение.

Конфиденциальность в сетевом представлении (КСП) - время между входом сигнала в узел/квазиподсеть и выходом из него/неё.

### 5.3.2. Алгоритм агрегирования.

Целевой функцией является минимальное время доступа извне (через открытые узлы, с учётом времени доступа извне к самим открытым узлам) к серверу. Она считается путём суммирования КСП квазиподсети, непосредственно содержащей открытый узел, КСП квазиподсети, непосредственно содержащей сервер, и КСП всех узлов на кратчайшем пути между этими квазиподсетями.

### 5.3.3. Примеры вычисления.

В простейшем случае КСП маршрутизатора задаётся формулой, где- длина пароля административной учётной записи маршрутизатора,- объём алфавита, из которого берутся символы для пароля, а- длительность единичной несупешной попытки авторизации. При закрытии некоторых портов маршрутизатора его КСП может быть задана формулой, где - доля незакрытых портов маршрутизатора.

### 5.3.4. Введение нормы.

Не требуется.

# 6. Методология построения реальной сети как продукта модели.

Итак, сформулируем пошаговый алгоритм построения сети, отвечающей полученным от пользователя требованиям информационной безопасности, от начала до конца:  
1. Построить модель сети, как описано в разделе 2.  
2. Примить методы, описанные в разделах 3. и 4., к полученной модели.  
3. На основе полученного общего представления с вычисленными оптимальными свойствами конечных узлов, коммутаторов, маршрутизаторов и связей между узлами подобрать конкретные экземпляры коммутаторов и маршрутизаторов, определённые виды кабелей, технику для размешения в конечных узлах, обладающие этими оптимальными свойствами. (В данной версии модели мы не рассматриваем возможность несуществования конкретных экземпляров, соответствующих оптимальным свойствам.)  
4. Настроить коммутаторы и маршрутизаторы для осуществления топологии сети, содержащейся в общем представлении (включая настройку VLAN-ов).  
5. Настроить сетевой экран на маршрутизаторах в соответствии с конфигурацией глобального сетевого экрана и встроенных сетевых экранов.

# 6. Заключение.

Поставленная задача по созданию типовой схемы ЛВС и разработки её математической модели была успешно выполнена.

С учётом отсутствия в литературе методологии количественного оценивания аспектов безопасности ЛВС (целостности и конфиденциальности) были разработаны собственные методы теоретической количественной оценки безопасности компонентов ЛВС и сети в целом.

На основе разработанных методов количественного анализа ЛВС предложен алгоритм оптимизации свойств компонентов сети.

В дальнейшем планируется получить количественную оценку критериев безопасности конкретных типов устройств и связей (вычисление параметров устройств, которые влияют на целевые функции, и установление характера этой зависимости), пользуясь предложенной методологией количественного анализа.

Также планируется описать вычислительную часть алгоритма оптимизации (подобрать подходящие к постановке задачи операторы генетического алгоритма).