На правах рукописи

Никонов Вячеслав Игоревич

# МЕТОДИКА ЗАЩИТЫ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ ТРАФИКА

05.13.19 – Методы и системы защиты информации, информационная безопасность

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени
кандидата технических наук

Томск 2010

Работа выполнена в ГОУ ВПО «Омский государственный технический университет»

Научный руководитель: доктор технических наук профессор Файзуллин Рашит Тагирович

Официальные оппоненты: доктор физико-математических наук Тимченко Сергей Викторович (Томский государственный университет систем управления и радиоэлектроники)

кандидат технических наук доцент Новиков Сергей Николаевич (Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск)

Ведущая организация: Омский государственный университет путей сообщения

Защита состоится « 29 » декабря 2010 г. в 12:30 часов на заседании диссертационного совета Д212.268.03 при Томском государственном университете систем управления и радиоэлектроники по адресу: 634050, г. Томск, пр. Ленина, 40.

С диссертацией можно ознакомиться в библиотеке Томского государственного университета систем управления и радиоэлектроники по адресу: г. Томск, пр. Ленина, 40.

Автореферат разослан «____» ноября 2010 г.

Ученый секретарь
Диссертационного совета

Р.В. Мещеряков

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность работы.** Развитие информационных технологий ставит актуальные задачи повышения надежности функционирования компьютерных сетей. Для решения таких задач необходимы исследования существующих сетевых протоколов, сетевых архитектур, разработка способов повышения безопасности при передаче информационных ресурсов по сети.

Выбор в пользу беспроводных технологий позволяет получить преимущества в скорости, мобильности. Появление нового класса широкополосных беспроводных сетей с ячеистой структурой (меш-сети) позволило достичь значительного увеличения зоны информационного покрытия. Основным достоинством данного класса сетей является наличие особых устройств – меш-порталов, позволяющих интегрировать в меш-сеть другие беспроводные сети (WiMAX, Wi-Fi, GSM) и Интернет, а значит, и предоставить пользователю всевозможные сервисы этих сетей.

К недостаткам меш-технологии можно отнести тот факт, что протоколы маршрутизации меш-сети весьма специфичны, а их разработка – сложная задача с множеством критериев и параметров. При этом существующие протоколы требуют значительных доработок в вопросах повышения безопасности и надежности передачи информации.

Сетевые атаки, сбои и отказы сетевого оборудования – основные факторы, влияющие на безопасность передачи информации в распределенных беспроводных сетях. Проблемой обеспечения безопасности передачи информации в распределенных беспроводных сетях занимались I. Akyildiz, W.Wang, X.Wang, T. Dorges, N. Ben Salem. Под обеспечением безопасности передачи информации в компьютерной сети понимается защита ее конфиденциальности, целостности и доступности.

Среди методов обеспечения доступности информации в беспроводных сетях исследователями выделяется комбинирование различных методов контроля, дублирования, резервирования. Целостность и конфиденциальность информации в беспроводных сетях обеспечивается методами построения виртуальных каналов, основанных на применении криптографических инструментов.

Общий недостаток данных методов – снижение производительности сети, связанное с требованиями к дополнительной обработке передаваемой информации. Указанный недостаток особенно критичен для передачи цифровой видеоинформации. Кроме того, совершенствование методов криптоанализа все более снижает надежность существующих криптоалгоритмов.

Из вышесказанного следует вывод о необходимости разработки новых способов защиты информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак. В связи с этим тема работы является актуальной и практически важной.

**Целью** диссертационной работы является разработка методики защиты информации при передаче в распределенных беспроводных сетях, основанной

на применении алгоритма динамической маршрутизации трафика в условиях воздействия преднамеренных атак.

**Задачи работы**

1. Анализ рекомендаций стандартов IEEE 802.11 по защите информации в распределенных беспроводных сетях.
2. Исследование алгоритмов динамической маршрутизации трафика в распределенных сетях.
3. Исследование методов защиты информации в распределенных беспроводных сетях.
4. Исследование видов атак в распределенных компьютерных сетях, анализ специфики атак в беспроводных сетях.
5. Разработка алгоритма динамической маршрутизации информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак.
6. Разработка на базе алгоритма приложения «маршрутизируемый сервис», реализующего методику защиты информации при передаче в распределенных беспроводных сетях.
7. Реализация программных модулей «маршрутизируемого сервиса» передачи информации.
8. Исследование вариантов воздействия сетевых атак на «маршрутизируемый сервис». Вычисление оценок успешных реализаций сетевых атак на передаваемую информацию в случае применения «маршрутизируемого сервиса».
9. Разработка алгоритма генерации потока сетевых атак.
10. Разработка прототипа «маршрутизируемого сервиса» для экспериментальной проверки предложенной методики защиты.

**Объектами исследования** являются компьютерные сети, распределенные беспроводные сети с ячеистой структурой (меш-сети), процессы передачи информации и процессы реализации различных видов атак на передаваемую информацию и сетевые устройства в распределенных беспроводных сетях.

**Предметы исследования:** стандарты группы IEEE 802.11, сетевые атаки, методы защиты информации в беспроводных сетях, алгоритмы динамической маршрутизации трафика в беспроводных сетях.

**Методы исследований.** В диссертационной работе используются методы математического моделирования, теории графов, теории множеств, теории вероятности и математической статистики. Для подтверждения полученных теоретических результатов проведены экспериментальные исследования и моделирование, с использованием сред программирования Visual Basic Script, Windows Management Instrumentarium, Shell, Awk.

**Достоверность** научных положений, выводов и рекомендаций подтверждается корректной постановкой задач, строгостью применяемого математического аппарата, результатами численного моделирования, положительными ре-

зультатами апробации программы, реализующей предложенную методику защиты информации при передаче в беспроводных сетях.

**Научная новизна.** В диссертационной работе получены следующие научные результаты.

1. Предложена методика защиты информации в распределенных беспроводных сетях, основанная на применении приложения «маршрутизируемый сервис».
2. Разработан алгоритм динамической маршрутизации информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак.
3. Описаны варианты реализации воздействия на разработанную систему. Даны оценки успешным реализациям сетевых атак на передаваемую информацию в случае применения «маршрутизируемого сервиса». Разработан алгоритм генерации потока сетевых атак.
4. Реализованы программные модули прототипа «маршрутизируемого сервиса» Произведена апробация прототипа в распределенной сети.

**Практическая значимость** подтверждена апробацией прототипа разработанной системы в распределенной сети. Результаты диссертационного исследования отмечены дипломом II-степени на IX Всероссийском конкурсе студентов и аспирантов по информационной безопасности «SIBINFO-2009».

Разработанная методика прошла внедрение в системы передачи информации ОАО «Омскводоканал и ГОУ ВПО «Омский государственный технический университет». Результаты диссертационной работы используются в учебном процессе ГОУ ВПО «Омский государственный технический университет».

Предлагаемая в диссертации методика может использоваться в качестве базы для дальнейших исследований.

**Апробация работы.** Результаты работы представлялись на научных конференциях и семинарах.

1. IX Всероссийский конкурс студентов и аспирантов по информационной безопасности «SIBINFO-2009», диплом II-степени. (2009, г. Томск).
2. VIII Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография – SYBECRYPT-09» (2009, г. Омск).
3. VII Международная научно-техническая конференция «Динамика систем, механизмов и машин» (2009, г. Омск).
4. IV Научно-практическая конференция молодых специалистов западно-сибирского банка сбербанка России «Современный опыт использования информационных технологий в банковском бизнесе» (2008, г. Тюмень).
5. Всероссийская научно-техническая конференция «Россия молодая: передовые технологии в промышленность» (2008, г. Омск).
6. Конференция-конкурс «Технологии Microsoft в теории и практике программирования» (2008, г. Новосибирск).

**Публикации.** Результаты диссертации отражены в 15 публикациях, в том числе в двух публикациях в изданиях, рекомендованных ВАК.

**Структура и объём работы.** Диссертационная работа состоит из введения, трех глав, заключения, списка литературы и трех приложений. Общий объем работы составляет 116 страниц, в том числе 26 рисунков и 3 таблицы. Список литературы насчитывает 82 наименования.

**Личный вклад**

Все исследования, изложенные в диссертационной работе, проведены автором в процессе научной деятельности. Все результаты, выносимые на защиту, получены автором лично, заимствованный материал обозначен в работе ссылками.

**Основные положения, выносимые на защиту**

1. Методика защиты информации в распределенных беспроводных сетях, основанная на использовании приложения «маршрутизируемый сервис».
2. Алгоритм динамической маршрутизации информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак.
3. Оценки успешных реализации сетевых атак на передаваемую информацию в случае применения «маршрутизируемого сервиса». Алгоритм генерации потока сетевых атак.
4. Программная реализация модулей «маршрутизируемого сервиса» передачи информации и экспериментальная проверка разработанной методики.

## СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность исследуемой в диссертации проблемы, формулируются основные цели и задачи исследования. Обосновывается научная новизна и значимость работы.

В первой главе анализируются рекомендации стандартов IEEE 802.11 по обеспечению безопасности передачи информации в беспроводных сетях. Исследуются основные виды уязвимости компьютерных сетей, раскрывается специфика уязвимостей беспроводных сетей. Рассматриваются существующие технологии защиты информации в распределенных беспроводных сетях, анализируются их достоинства и недостатки. В результате проведенного обзора делается вывод, что существующие методы защиты является узкоспециализированными при противодействии угрозам информации. Также большинство методов не применимы в силу различных ограничений для обеспечения безопасности передачи ресурсоемких видов информации, в том числе потокового видео. Данный факт предопределяет необходимость разработки и реализации специализированных методов защиты информации при передаче в распределенных беспроводных сетях, направленных на решение поставленных задач.

В заключение главы формулируются цели и задачи диссертационной работы.

Во второй главе приводится описание разработанной методики защиты информации при передаче в распределенных беспроводных сетях и её главных параметров: доверенных серверов, алгоритма динамической маршрутизации, приложения «маршрутизируемый сервис», оценок успешной реализации преднамеренных атак, алгоритма генерации потока сетевых атак.

Вводятся следующие обозначения.

$S_M$ – «маршрутизируемый сервис» - клиент-серверное приложение, позволяющее пользователю передавать информацию специфичным маршрутом.

$S_M = \{S_{MS}, S_{MC}\}$.

$S_{MC}$ – клиентская часть $S_M$, которая устанавливается на компьютерах пользователей и предоставляет диалог для инициализации процесса передачи информации с помощью «маршрутизируемого сервиса».

$S_{MS}$ – серверная часть $S_M$, которая устанавливается на доверенном сервере и выполняет динамическую маршрутизацию информации, поступающего на этот сервер.

$S_{MS} = \{F_S, F_S^{дост}, M, f\}$.

$F_S = \{F_{S1}, F_{S2}, ..., F_{Si}, ..., F_{SF}\}$ – множество доверенных серверов сети. Под доверенным сервером понимается многофункциональный сервер распределенной беспроводной сети, к которому нарушитель не имеет доступа.

$F = |F_S|$ - количество доверенных серверов сети.

$F_S^{дост} = \{F_{S1}^{дост}, F_{S2}^{дост}, ..., F_{Si}^{дост}, ...., F_{SF}^{дост}\}$ – множество, описывающее количество доступных доверенных серверов в начальный момент времени $t_0$, а затем через интервалы времени, равные τ. $F_{Si}^{дост}$ – количество доступных доверенных серверов для $F_{Si}$, $i \in [1; F]$.

$M = \{M_1, M_2, ..., M_i, ..., M_F\}$ – множество матриц маршрутизации. Матрица маршрутизации $M_i$ формируется на сервере $F_{Si}$ в начальный момент времени $t_0$, а затем переформировывается через интервалы τ, $i \in [1; F]$. Каждая матрица $M_i \in F_{Si}$ содержит элементы $m_{kj}$, характеризующие доступность доверенных серверов относительно друг друга из $F_{Si}$, $k \in [1, F], j \in [1, F]$.

$f$ – параметр, определяющий количество используемых доверенных серверов на всем маршруте от отправителя до получателя в течение одного сеанса (размер «кластера сеанса передачи»).

Предлагаемая методика представлена на рис. 1 в виде IDEF диаграммы.

Методика включает последовательность следующих действий.

1. Анализ топологии распределенной сети. Выбор устройств сети для роли «доверенный сервер».
2. Установка и настройка $S_{MS}$ на доверенных серверах, $S_{MC}$ на рабочих станциях.
3. Выбор параметров передачи $S_{MC}$.
4. Передача данных через доверенные сервера на основе алгоритма динамической маршрутизации.
5. Прием данных получателем, сбор статистики по построенным маршрутам, оценки реализаций возможных атак.

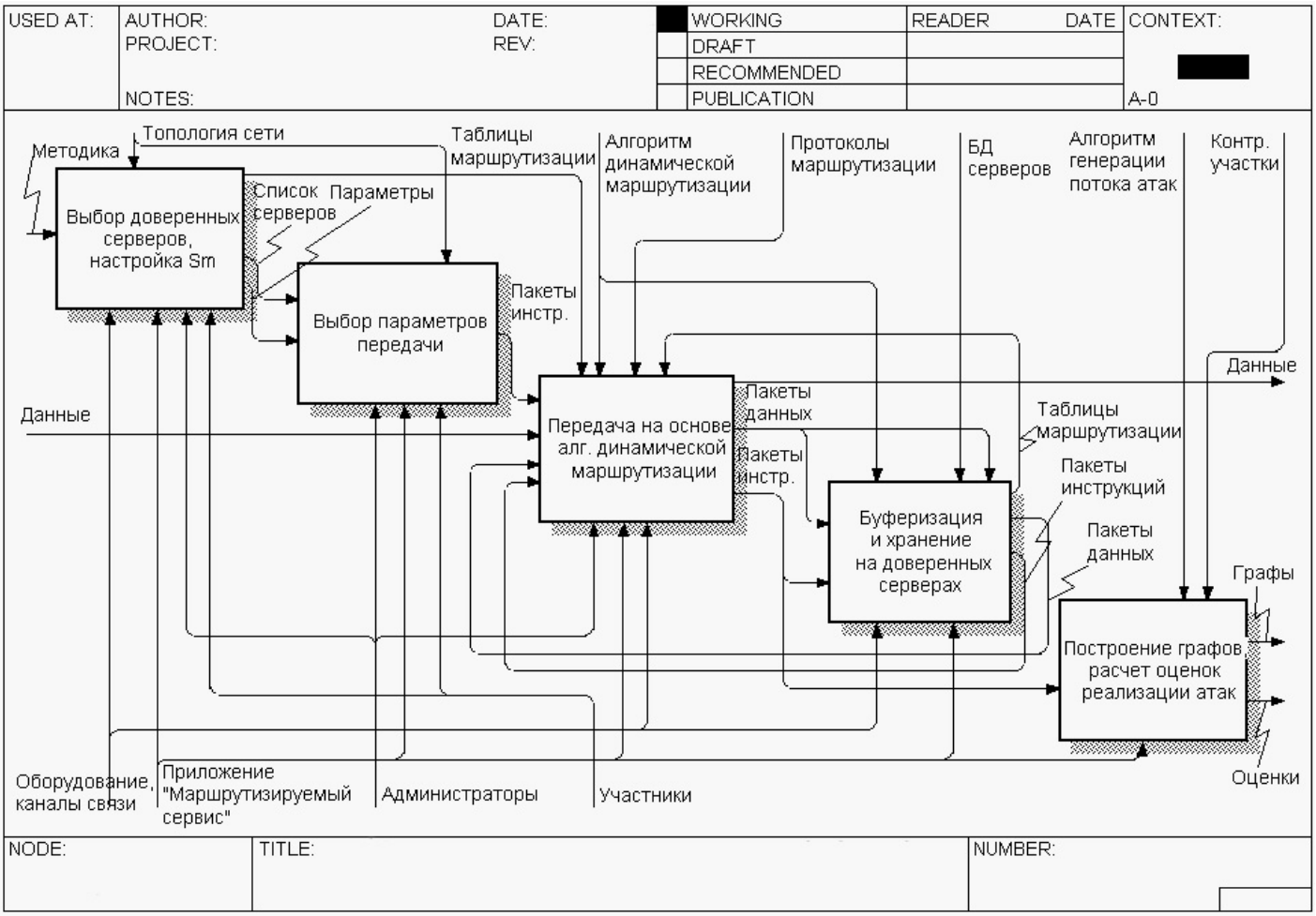



Рис. 1. Методика защиты информации в распределенных беспроводных сетях.

Главной особенностью предложенного подхода является применение динамической маршрутизации для цели защиты информации.

Разработанный алгоритм динамической маршрутизации информации в распределенных беспроводных сетях, описывается следующими этапами.

Шаг 1. Вычисление элементов множеств $M$ и $F_S^{дост}$ в начальный момент времени $t_0$.

Шаг 2. Инициализация передачи. При поступлении запроса $S_{MC}$ на инициализацию сеанса передачи данных выполнить следующие действия:

2.1. запросить значение параметра $f$;

2.2. создать пакет инструкций, содержащий ip-адрес отправителя, ip-адрес получателя, значение $f$ и раздел «доверенные сервера»;

2.3. используя операцию рандомизации, получить псевдослучайное число $k$;

2.4. проверить доступность $F_{Sk}$ , если сервер недоступен – вернуться к п.2.3;

2.5. сформировать пакет данных и промаркировать его как пакет $S_M$;

2.6. отправить пакет данных и пакет инструкций на доверенный сервер $F_{Sk}$. Если требуется дальнейшая передача данных – вернуться к п.2.5;

2.7. завершить работу $S_{MC}$.

Шаг 3. Динамическая маршрутизация на доверенном сервере $F_{Si}$:

3.1. переформировать матрицу маршрутизации в случае, если разность текущего времени и времени последнего изменения $M_i$ больше $t$. При получении пакетов $S_M$ - перейти к п.3.2;

3.2. открыть полученный пакет инструкций, в раздел «доверенные сервера» добавить ip-адрес $F_{Si}$;

3.3. если количество записей в разделе «доверенные сервера» равно $f$, отправить пакеты данных, относящиеся к данному пакету инструкций, на ip-адрес получателя и вернуться на п.3.1;

3.4. используя операцию рандомизации, получить псевдослучайное число $k$;

3.5. проверить доступность $F_{Sk}$ , если сервер недоступен – вернуться к п.3.4;

3.6. проверить наличие информации о $F_{Sk}$ в разделе «доверенные сервера»; если $F_{Sk}$ присутствует в данном разделе – вернуться к п.3.4;

3.7. отправить пакет инструкций и относящиеся к нему пакеты данных на доверенный сервер $F_{Sk}$; вернуться на п.3.1.

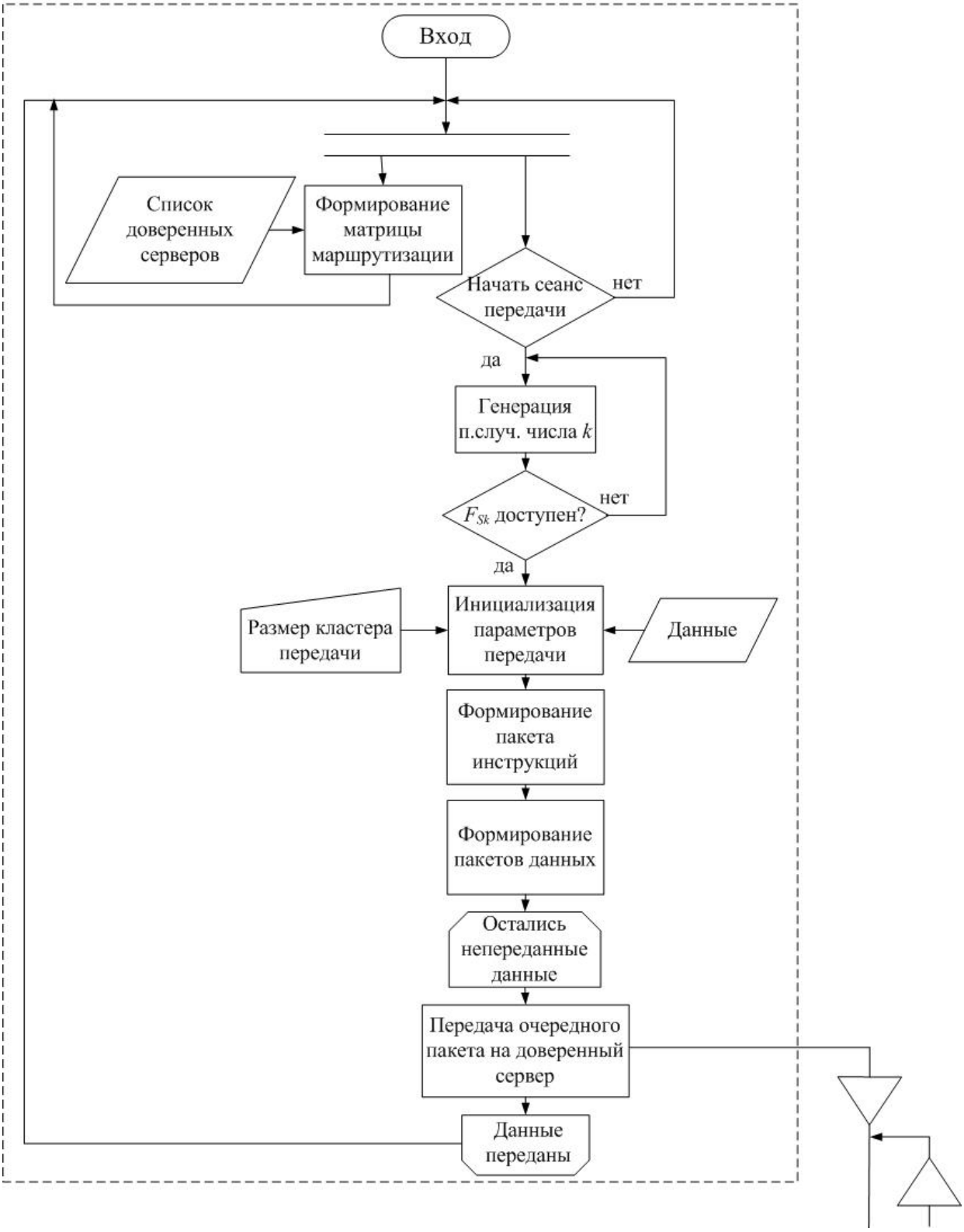
Шаг 4. Получение пакета данных и пакета инструкций $S_{MC}$, определяемым ip-адресом получателя.

Согласно ГОСТ 19.701-90 Единой системы программной документации схему алгоритма можно представить в следующем виде (рис. 2).

Повышение защищенности информации в распределенных беспроводных сетях при использовании $S_M$ достигается за счет повышения защиты ее конфиденциальности, целостности и доступности. Далее проводится анализ представленной методики.

Для достижения поставленной цели исследуется множество преднамеренных сетевых атак. Предлагается разбить все типичные сетевые атаки, которым может подвергнуться «маршрутизируемый сервис» на два класса: атаки на трафик между «смежными» серверами и атаки непосредственно на доверенные сервера $F_S$. Понятие «смежности» определяется динамически для каждого сеанса передачи.

В работе получена оценка реализации атаки первого класса $R_{A1}$, когда контролируется участок между доверенными серверами $F_{Sj}$ и $F_{Sj+1}$. (рис. 3) При неизвестном пространственном расположении $F_{Si}$ считаем атаку успешной, если при работе сервиса $S_M$ передатчики $F_{Sj}$ и $F_{Sj+1}$ были выбраны на $i$ и $i$+1 этапе передачи.


Вход
Список доверенных серверов
Формирование матрицы маршрутизации
Начать сеанс передачи
нет
да
Генерация п.случ. числа $k$
$F_{Sk}$ доступен?
нет
да
Размер кластера передачи
Инициализация параметров передачи
Данные
Формирование пакета инструкций
Формирование пакетов данных
Остались непереданные данные
Передача очередного пакета на доверенный сервер
Данные переданы

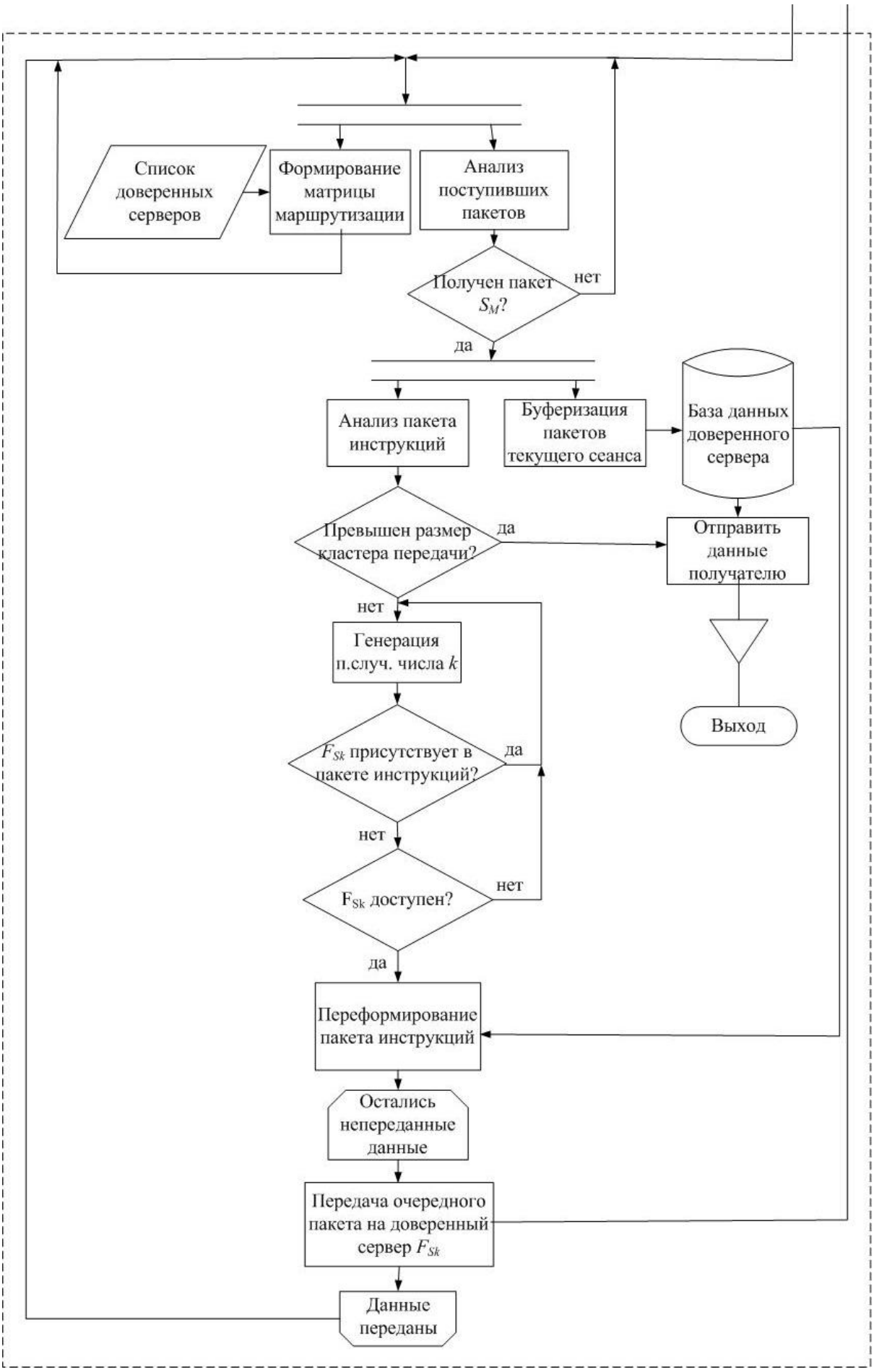



Рис. 2. Блок-схема разработанного алгоритма динамической маршрутизации

$$R_{A1}=\begin{cases}\dfrac{2}{F_{S0}^{дост}\cdot\left(F_{S0}^{дост}-1\right)}, f=2\\ \dfrac{2}{F_{S0}^{дост}\cdot\left(F_{S0}^{дост}-1\right)}+\sum\limits_{i=1}^{f-2}\left[\left(\dfrac{2}{F_{S0}^{дост}-i}\cdot\dfrac{1}{F_{S0}^{дост}-i-1}\right)\cdot\left(\prod\limits_{j=1}^{i}\dfrac{F_{S0}^{дост}-j-1}{F_{S0}^{дост}-j+1}\right)\right], f>2\end{cases}. \quad (1)$$

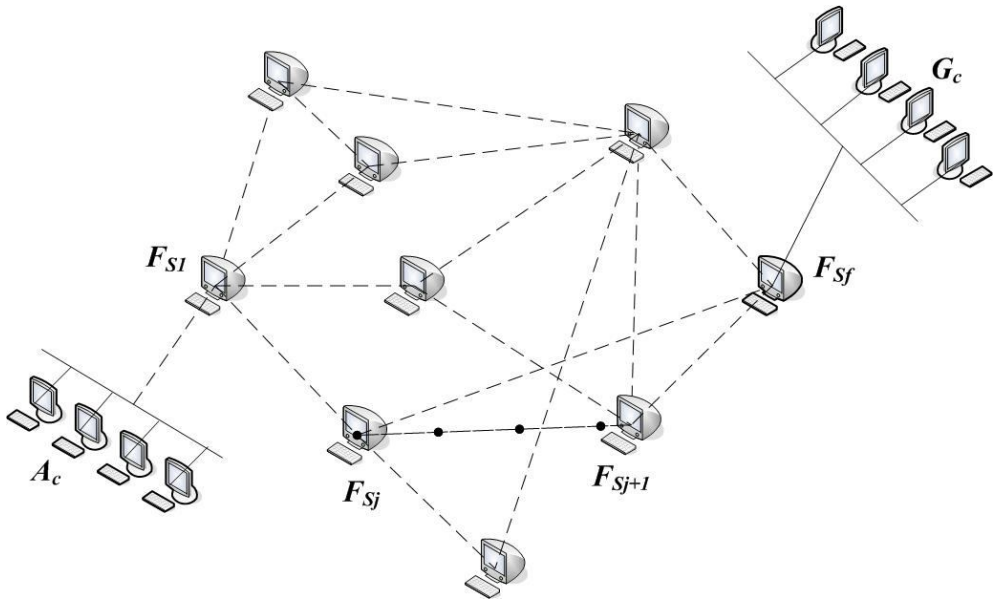



Рис. 3. Возможное представление беспроводной распределенной сети с контролируемым нарушителем участком $F_{Sj}F_{Sj+1}$.

При некоторых значениях параметров оценка (1) представляется в виде:

$$R_{A1}=O\left(\frac{1}{F^2}\right). \quad (2)$$

Второй, более широкий, класс атак представляется в виде ординарного потока событий, т.е. последовательности событий, наступающих одно за другим в случайные промежутки времени.

Обозначим, $q$ – количество успешно атакованных серверов в единицу времени (интенсивность). Тогда оценка реализации атак на $m$-доверенных серверов за время $t$ описывается распределением Пуассона.

$$R_{A2}(m,t)=\frac{\lambda^m}{m!}\mathrm{e}^{-\lambda}=\frac{(q\cdot t)^m}{m!}\mathrm{e}^{-(q\cdot t)}=\frac{\left(\sum\limits_{i=1}^{k}(p_i\cdot h_i)\cdot t\right)^m}{m!}\mathrm{e}^{-\sum\limits_{i=1}^{k}(p_i\cdot h_i)\cdot t}. \quad (3)$$

Параметр $k$ в формуле (3) определяет число различных видов сетевых атак. Значение $q$ возможно оценить с помощью специальных Систем Обнаружения Вторжений (СОВ-сенсоров). СОВ-сенсоры рассматривались в первой главе. Они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин. Сенсоры регистрируют различные виды сетевых атак на наблюдаемые сервера. Но, как показали ре-

зультаты использования СОВ-сенсоров, практически невозможно дать точную оценку $q$, так как ее величина зависит от многих факторов: времени наблюдения, расположения сервера, функционального назначения сервера и др.

Для исследования этой проблемы был разработан алгоритм генерации потока атак, не зависящего от вышеперечисленных факторов (рис. 4). Для данной модели задаются параметры.

$F_S = \{F_{S1}, F_{S2}, \ldots, F_{Sj}, \ldots, F_{SF}\}$ – множество доверенных серверов сети.

$F = |F_S|$ - количество доверенных серверов сети.

$t_a$ – время действия одного вида атаки на доверенный сервер.

$u_1$ – период повтора атаки.

$u_2$ – период блокирования доверенного сервера.

$k$ – число видов атак.

$i, j, t$ – вспомогательные переменные.

Вводятся следующие функции и процедуры.

ТекВремя() – функция, возвращающая текущее время в формате «dd.mm.yyyy hh24:mi:ss».

ГенСлуч($x$) – функция, генерирующая псевдослучайное целое число с помощью операции рандомизации, принадлежащее интервалу [1;$x$], $x$ >= 1;

РазБлок($F_j$) – процедура, переводящая сервер $F_j$ в режим «доступен».

$A_i(F_j)$ – функция распределения дискретной случайной величины «результат атаки на сервер $F_j$» с вероятностью принять значение 1 (атака успешна) равной $p_i$ и вероятностью принять значение 0 (атака неудача) равной 1- $p_i$.

Пауза($t$) – процедура, реализующая ожиние на время $t$;

СостСерв($F_j$) – функция, возвращающая статус сервера $F_j$ (доступен - 0; блокирован - 1);

Блок($F_j$, $x$) – функция, переводящая сервер $F_j$ в режим «блокирован» и возвращающая текущее время в формате «dd.mm.yyyy hh24:mi:ss» переменную $x$.

Блок-схема моделирует воздействие потока атак на доверенные сервера (рис. 4).

Описание схемы.

С помощью операции рандомизации выбираются один из доверенных серверов сети и сетевая атака одного из видов. Производится эксперимент $A_i(F_{Sj})$ – «атака на сервер $F_{Sj}$», определяемый дискретной случайной величиной с распределением «вероятность принять значение 1 (успех) равна $p_i$, вероятность принять значение 0 (неудача) равна 1- $p_i$», $i \in [1, k]$. В случае успеха, сервер блокируется и становится недоступным на время $u_2$. В процессе исследований с помощью предложенного алгоритма произведены попытки экспериментальных оценок значений $p_i$ и $h_2$, дальнейшая оценка данных параметров представляет интерес как независимое исследование.

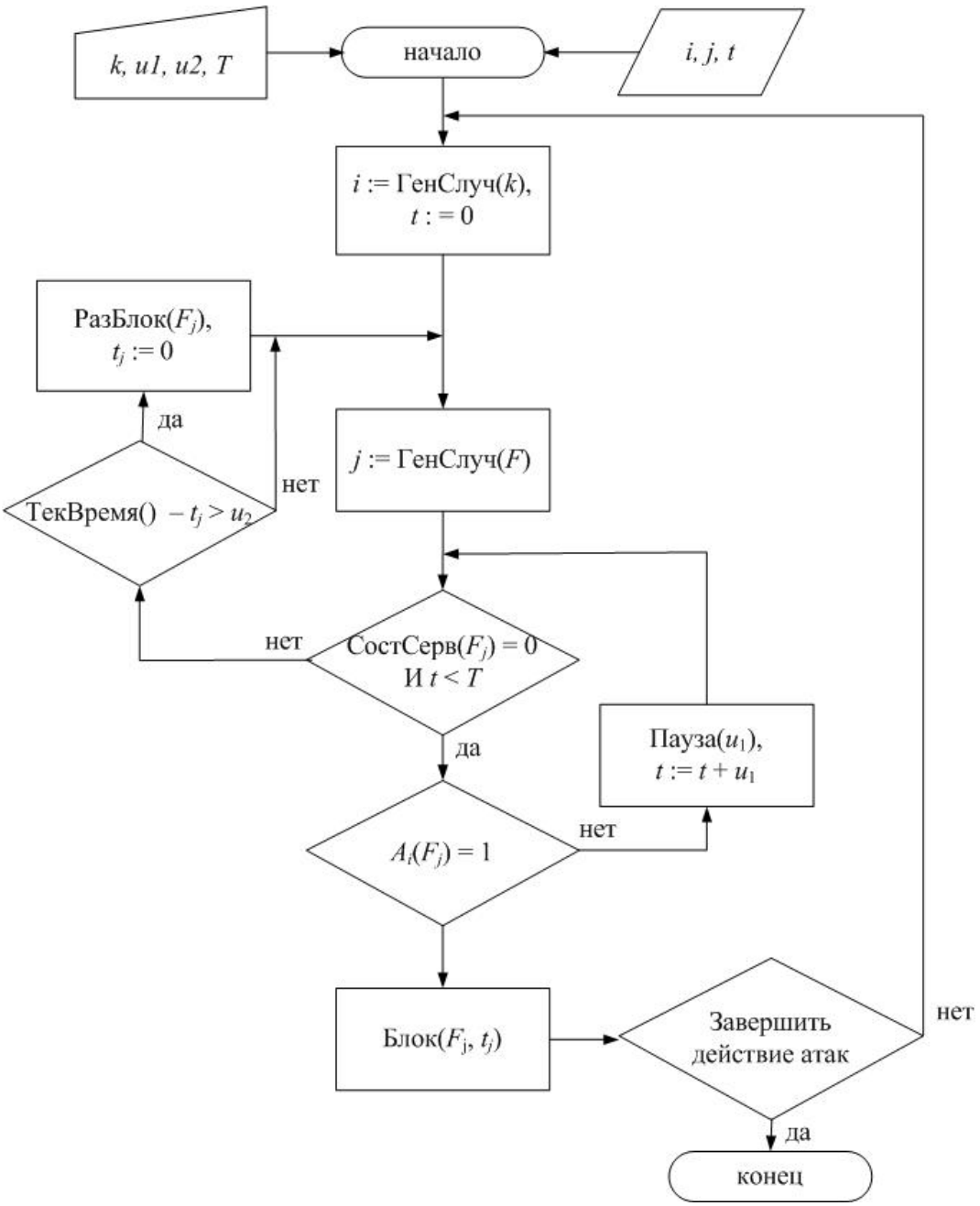



Рис. 4. Блок-схема модели потока атак на доверенные сервера

Полученные оценки реализации сетевых атак показывают, что применение приложения «маршрутизируемый сервис» позволяет повысить безопасность передачи информации в распределенных беспроводных сетях. Повышение защищенности информации в распределенных беспроводных сетях при использовании $S_M$ достигается за счет повышения защиты ее конфиденциальности, целостности и доступности. Целостность и конфиденциальность передаваемой информации обеспечивается уменьшением вероятности реализации сетевых атак на контролируемых участках следования трафика в случае применения «маршрутизируемого сервиса». Доступность обосновывается стойкостью системы к блокированию нарушителем одного или нескольких доверенных серверов. В случае сбоя в работе одного или нескольких доверенных серверов, «маршрутизируемый сервис» моментально перестраивает маршрут следования трафика до того времени, пока работоспособность доверенных серверов не вос-

становится. Следует также еще одно важное качество разработанного приложения - каждый из доверенных серверов может динамически вносить изменения в маршрут следования трафика.

В третьей главе представлена структура программного комплекса «маршрутизируемый сервис» и содержится описание эксперимента. В соответствии с задачами исследований была предложена следующая структурная схема программного комплекса.

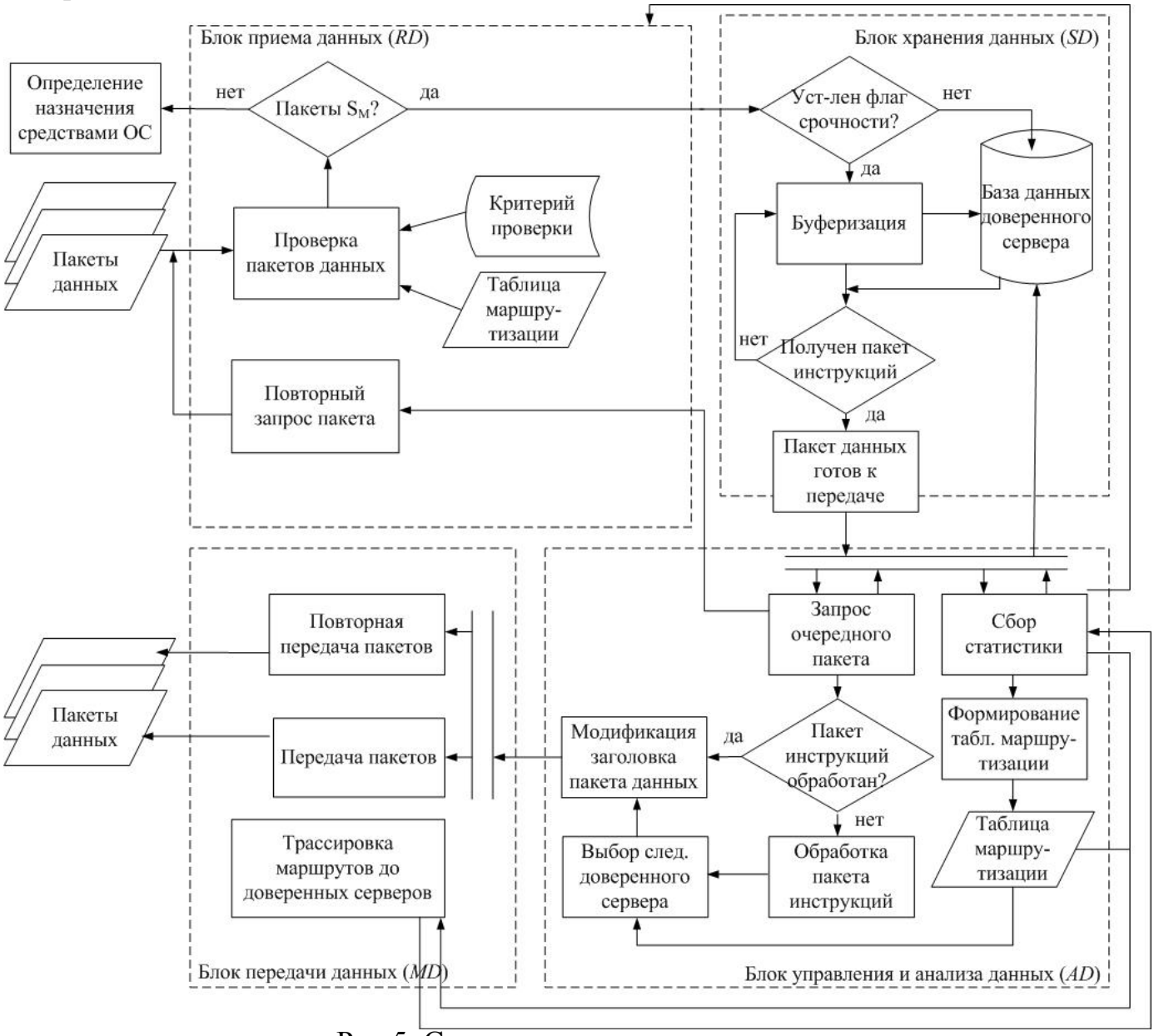



Рис 5. Структура программного комплекса.

Предлагаемая в работе схема программного комплекса «маршрутизируемый сервис» содержит четыре основных блока. Каждый блок выполняет определенное функциональное назначение.

1. Блок *RD* – из потока IP-пакетов выделяет пакеты с маркером $S_M$. Передает эти пакеты блоку *SD*;
2. Блок *SD* – база данных, содержит сведения о пакетах $S_M$, обработанных доверенным сервером $F_{Si}$, $i \in [1; F]$. В случае необходимости буферизирует пакеты данных.

3. Блок *AD* – анализирует пакеты данных и инструкций, принятые от блока *SD*, добавляет информацию о текущем доверенном сервере $F_{Si}$, $i \in [1; F]$ в пакет инструкций. Передает блоку *MD* команды на передачу данных и трассировку доверенных серверов, формирует таблицу маршрутизации $M_i \in F_{Si}$, $i \in [1; F]$. Получает от *SD* информацию о новых доверенных серверах, появившихся в сети.
4. Блок *MD* – отправляет очередной пакет на один из выбранных доверенных серверов или в пункт назначения.

Эксперимент заключался в создании приложения «маршрутизируемого сервиса» с использованием сред программирования Visual Basic Script и Windows Management Instrumentarium. Работа приложения «маршрутизируемый сервис» опробована на беспроводной сети крупного предприятия, проведено 282 сеанса испытаний на семи доверенных серверах. Описание процесса тестирования «маршрутизируемого сервиса» приведено в диссертационной работе.

В связи с потребностью проведения большого числа испытаний и автоматической обработки результатов также реализован прототип «маршрутизируемого сервиса». Прототип представляет собой приложение, созданное в среде Borland C++, позволяющее генерировать топологии сетей, задавать контролируемые участки и осуществлять сеансы передачи (рис. 6а, б).

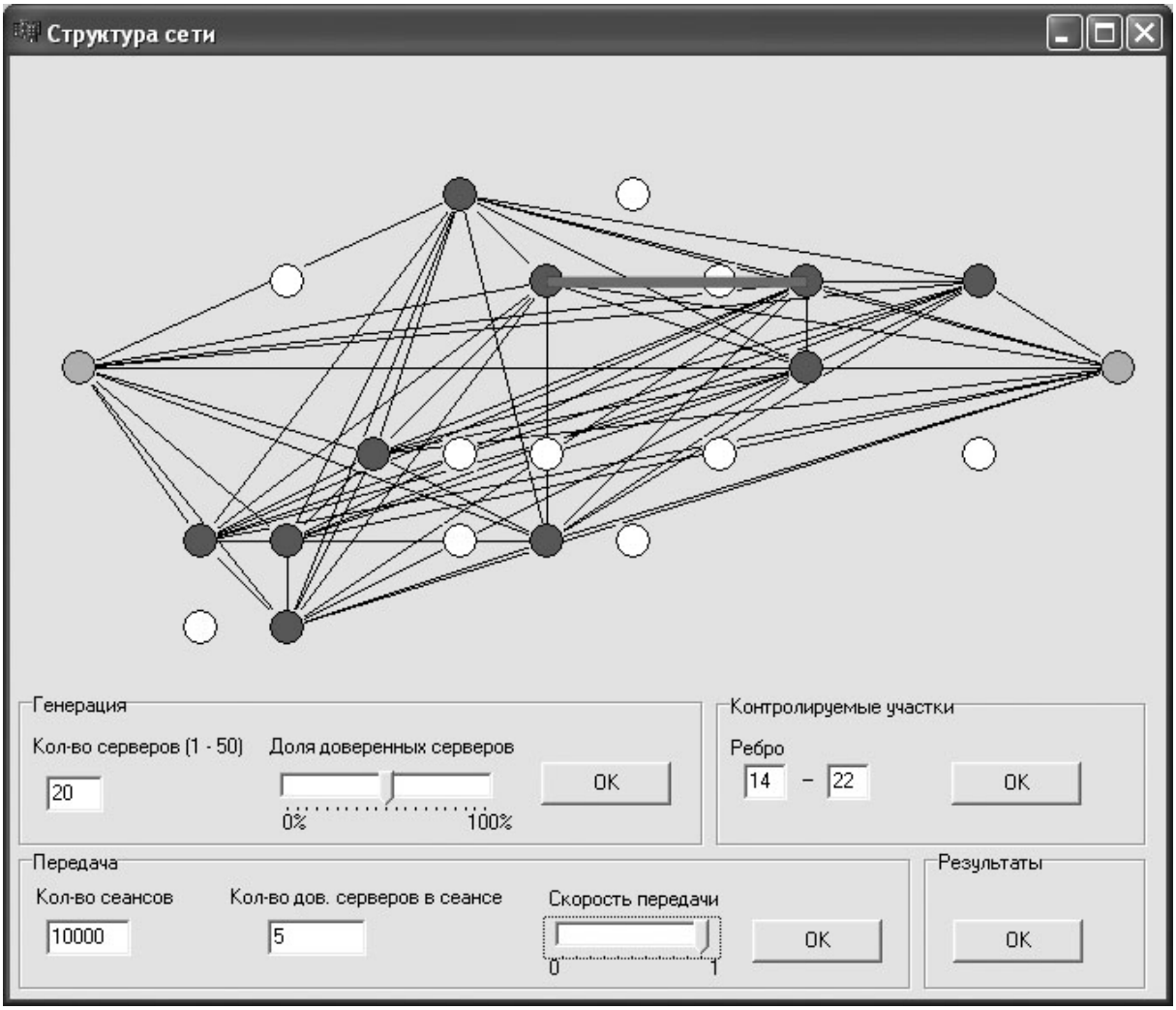


Рис.6а. Прототип «маршрутизируемого сервиса». Топология А.

На рис. 6а показана одна из возможных топологий сети, построенная прототипом приложения на основе 10-серверов (белый цвет), 10-доверенных серверов (черный цвет), отправителя и получателя (серый цвет). Ребро между доверенными серверами показывает наличие канала передачи данных ними.

Процесс тестирования состоял из следующих положений.

1. Топология сети содержит:

а) 10 доверенных серверов (топология А) (рис. 6а);

б) 26 доверенных серверов (топология Б) (рис. 6б).

2. В текущей топологии задается один контролируемый участок.

3. Для каждой топологии для вычисления оценки $R_{Acp}$ проводится пробная серия экспериментов, включающая 30 экспериментов по 10000 испытаний (сеансов передачи).

В течение одного сеанса передачи $S_M$ использует:

а) 5 доверенных серверов (топология А).

б) 5 доверенных серверов (топология Б).

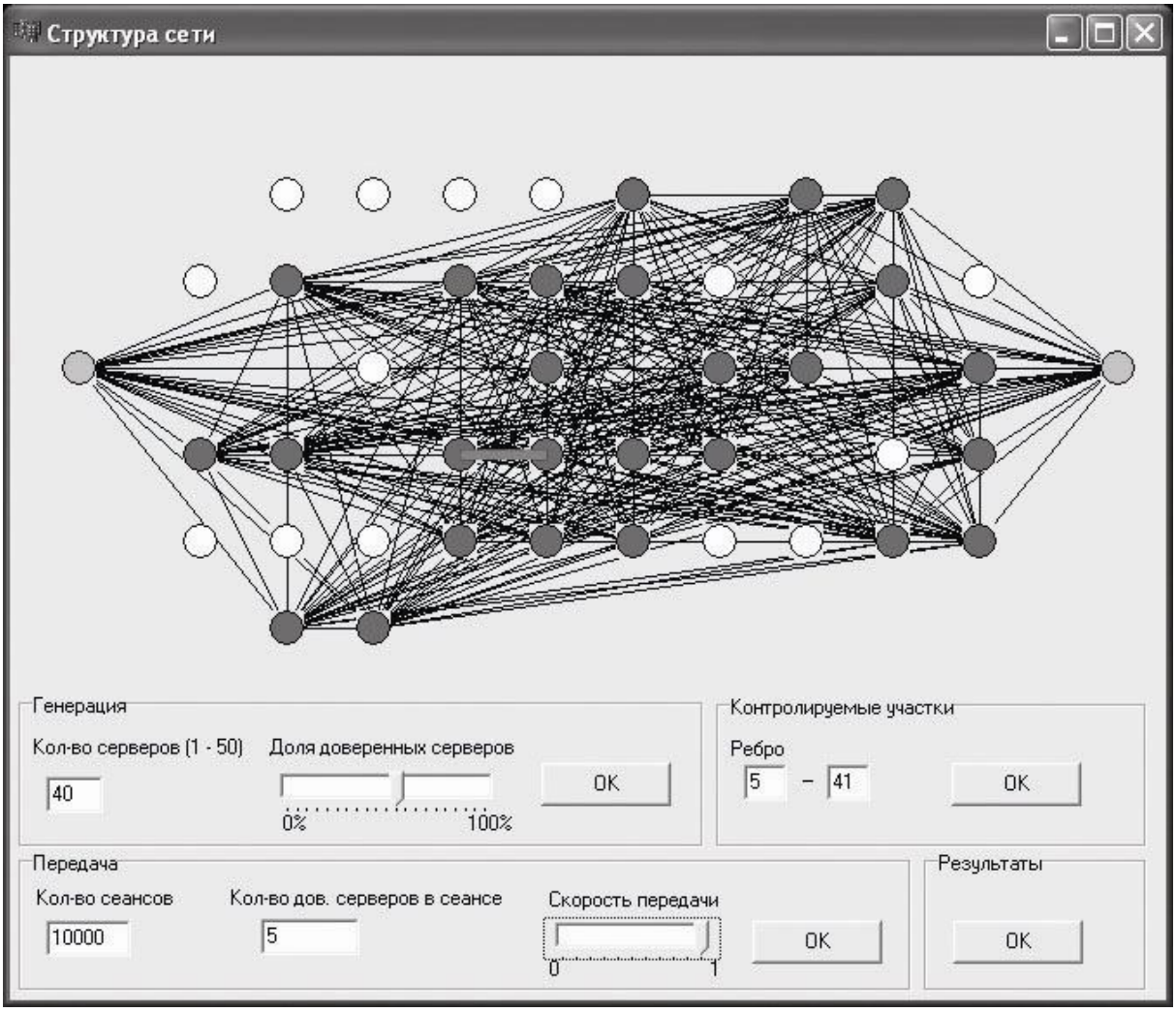



Рис.6б. Прототип «маршрутизируемого сервиса». Топология Б.

4. По результатам оценки $R_{Acp}$ вычисляется $N_{кр}(P_д,\varepsilon)$ – критическое значение необходимого количества испытаний в эксперименте. Доверительная вероятность принимается равной $P_д = 0{,}95$, доверительный интервал $\varepsilon = 0{,}001$.

5. Проводится эксперимент, состоящий из $N_{кр}$ сеансов передачи. По результатам эксперимента вычисляется $R_{Апр.}$

6. Если колебание значения оценки $R_{Апр}$ относительно теоретической оценки $R_{Ат}$ меньше заданной точности, то экспериментальная оценка $R_{Апр}$ принимается достоверной.

В результате пробной серии экспериментов получена оценка реализации атак на контролируемом участке $R_{Ai}$. Данная оценка рассчитана по формуле (4).

$$R_{Ai} = \frac{N_K}{N}, \tag{4}$$

где $N_K$ – количество исходов (сеансов), содержащих контролируемый участок, $N$ – общее количество исходов (сеансов) в эксперименте, $i$ – номер эксперимента. Результаты 30 экспериментов представлены в сводной таблице (табл.1).

Средняя оценка реализации атаки на контролируемом участке будет равна для топологии А:

$$R_{A\,\text{срА}} = \frac{\sum_{i=1}^{30} R_{Ai}}{30} = 0{,}0888, \tag{5}$$

для топологии Б:

$$R_{A\,\text{срБ}} = \frac{\sum_{i=1}^{30} R_{Ai}}{30} = 0{,}0125. \tag{6}$$

Критическое значение необходимого количества испытаний в эксперименте вычислено согласно следствию из центральной предельной теоремы.

$$N_{кр} = \frac{R_{A\text{ср}} \cdot (1 - R_{A\text{ср}})}{\varepsilon^2} \cdot \left(F^{-1}(\text{Р}_{\text{д}})\right)^2, \tag{7}$$

где $F^{-1}$ – обратная функция Лапласа.

Из формулы (7), учитывая оценки (5) и (6), а также ε = 0,001 и табличное значение $\left(F^{-1}(0{,}95)\right)^2 = 3{,}84$, вычислены значения $N_{кр\,А}$ и $N_{кр\,Б}$:

$N_{кр\,А} = 310712$, $N_{кр\,Б} = 47400$.

$R_{Апр\,А}$ и $R_{Апр\,Б}$ вычислены по формуле (4) по результатам экспериментов с количеством испытаний $N_{кр\,А}$ и $N_{кр\,Б}$:

$$R_{A\text{пр А}} = \frac{N_K}{N_{\text{кр А}}} = \frac{27855}{310712} \approx 0{,}0896,$$

$$R_{A\text{пр Б}} = \frac{N_K}{N_{\text{кр Б}}} = \frac{582}{47400} \approx 0{,}0123.$$

Таблица 1

Сводная таблица по результатам эксперимента

| $i$ | $N_i$ | Топология А | | Топология Б | |
|---|---|---|---|---|---|
| | | $N_{Ki}$ | $R_{Ai}$ | $N_{Ki}$ | $R_{Ai}$ |
| 1 | 10000 | 869 | 0,0869 | 119 | 0,0119 |
| 2 | 10000 | 865 | 0,0865 | 145 | 0,0145 |
| 3 | 10000 | 884 | 0,0884 | 120 | 0,0120 |
| 4 | 10000 | 828 | 0,0828 | 118 | 0,0118 |
| 5 | 10000 | 876 | 0,0876 | 142 | 0,0142 |
| 6 | 10000 | 910 | 0,0910 | 129 | 0,0129 |
| 7 | 10000 | 857 | 0,0857 | 148 | 0,0148 |
| 8 | 10000 | 946 | 0,0946 | 124 | 0,0124 |
| 9 | 10000 | 880 | 0,0880 | 138 | 0,0138 |
| 10 | 10000 | 871 | 0,0871 | 122 | 0,0122 |
| 11 | 10000 | 895 | 0,0895 | 119 | 0,0119 |
| 12 | 10000 | 901 | 0,0901 | 148 | 0,0148 |
| 13 | 10000 | 921 | 0,0921 | 111 | 0,0111 |
| 14 | 10000 | 867 | 0,0867 | 137 | 0,0137 |
| 15 | 10000 | 960 | 0,0960 | 127 | 0,0127 |
| 16 | 10000 | 858 | 0,0858 | 127 | 0,0127 |
| 17 | 10000 | 872 | 0,0872 | 109 | 0,0109 |
| 18 | 10000 | 891 | 0,0891 | 118 | 0,0118 |
| 19 | 10000 | 881 | 0,0881 | 117 | 0,0117 |
| 20 | 10000 | 909 | 0,0909 | 122 | 0,0122 |
| 21 | 10000 | 854 | 0,0854 | 129 | 0,0129 |
| 22 | 10000 | 923 | 0,0923 | 125 | 0,0125 |
| 23 | 10000 | 911 | 0,0911 | 116 | 0,0116 |
| 24 | 10000 | 882 | 0,0882 | 113 | 0,0113 |
| 25 | 10000 | 926 | 0,0926 | 117 | 0,0117 |
| 26 | 10000 | 874 | 0,0874 | 131 | 0,0131 |
| 27 | 10000 | 870 | 0,0870 | 103 | 0,0103 |
| 28 | 10000 | 877 | 0,0877 | 133 | 0,0133 |
| 29 | 10000 | 924 | 0,0924 | 129 | 0,0129 |
| 30 | 10000 | 871 | 0,0871 | 113 | 0,0113 |

Для вычисления теоретической оценки реализации атаки на контролируемом участке воспользуемся формулой (1), приняв допущение, что все сервера работоспособны во время испытаний (параметры $|F_{Si}^{\,дост}| = F$).

$$R_{А\,т\,А} = \frac{2}{10 \cdot 9} + \sum_{i=1}^{3}\left[\left(\frac{2}{10-i} \cdot \frac{1}{10-i-1}\right) \cdot \prod_{j=1}^{i}\left(\frac{10-j-1}{10-j+1}\right)\right] = 0{,}0889 \qquad (8)$$

$$R_{А\,т\,Б} = \frac{2}{26 \cdot 25} + \sum_{i=1}^{3}\left[\left(\frac{2}{26-i} \cdot \frac{1}{26-i-1}\right) \cdot \prod_{j=1}^{i-1}\left(\frac{26-j-1}{26-j+1}\right)\right] = 0{,}0123 \qquad (9)$$

Колебание значения оценок $R_{Апр\ А}$ и $R_{Апр\ Б}$ относительно теоретических оценок $R_{Ат\ А}$ и $R_{Ат\ Б}$ меньше заданной точности ε = 0,001 поэтому можно сделать вывод о соответствии практических результатов теоретическим представлениям работы сервиса $S_M$ с доверительной вероятностью 0,95.

Результаты экспериментальных исследований подтвердили применимость разработанной методики. Данная методика прошла внедрение в системы передачи информации ОАО «Омскводоканал» и ГОУ ВПО «Омский государственный технический университет».

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В процессе исследований, выполненных в диссертационной работе, получены следующие результаты.

1. Проанализированы рекомендации стандартов IEEE 802.11 по защите информации в распределенных беспроводных сетях.
2. Исследованы алгоритмы динамической маршрутизации трафика в распределенных сетях.
3. Исследованы методы защиты информации в распределенных беспроводных сетях.
4. Построен алгоритм динамической маршрутизации информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак.
5. На базе алгоритма разработано приложение «маршрутизируемый сервис», реализующее методику защиты информации при передаче в распределенных беспроводных сетях.
6. Реализованы программные модули «маршрутизируемого сервиса».
7. Исследованы варианты воздействия сетевых атак на «маршрутизируемый сервис». Вычислены оценки успешных реализаций сетевых атак на передаваемую информацию в случае применения «маршрутизируемого сервиса».
8. Разработан алгоритм генерации потока сетевых атак.
9. Произведена экспериментальная проверка разработанной методики.

## ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ


1. **Никонов В.И. Маршрутизация в беспроводных сетях нового поколения // Системы управления и информационные технологии. Научно-технический журнал. – Воронеж: издательство «Научная книга», 2010. – №1.1(39). – С. 170-173.**
2. **Никонов В.И. Методы защиты информации в распределенных компьютерных сетях с помощью алгоритмов маршрутизации // Доклады Томского государственного университета систем управления и радиоэлектроники. Научный журнал. – Томск: издательство ТГУСУР, 2010. – № 1 (21) , часть 2. – С. 219-224.**
3. Никонов В.И. Вероятностная оценка трафика и информационной безопасности системы связи / В.И. Никонов, И.В. Никонов // Техника радиосвязи. – 2008. – №13. – С. 91-96.
4. Никонов В.И. Маршрутизируемый сервис передачи данных через распределенные сети // Материалы конференции - конкурса работ студентов, аспирантов и молодых ученых «Технологии Microsoft в теории и практике программирования» 1-2 марта 2008г. - Новосибирск: Академгородок, 2008. – С. 83-84.
5. Никонов В.И. Маршрутизируемый сервис передачи данных // Материалы Всероссийской научно-технической конференции «Россия молодая: передовые технологии в промышленность» 12-13 ноября 2008. – Омск: Омский государственный технический университет, 2008. – С. 80-84.
6. Никонов В.И. Организация видеоконференций между отделениями банка // Материалы IV научно-практической конференции «Современный опыт использования информационных технологий в банковском бизнесе» 13 декабря 2008 г. - Тюмень, 2008. – С. 46-49.
7. Никонов В.И. Вероятностный анализ информационной безопасности систем связи // Техника радиосвязи. Научно-технический сборник.- Омск: издательство Омского научно-исследовательского института приборостроения, 2009.- Выпуск 13. - С.112-115.
8. Никонов В.И. Передача данных через распределенные сети связи // Материалы региональной научно-практической конференции «Наука, образование, бизнес». – Омск: институт радиоэлектроники, сервиса и диагностики, 2009. – С. 206-208.
9. Никонов В.И. Маршрутизируемый сервис передачи данных через распределенные сети // Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2009» 12-15 мая 2009г. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2009. – Часть 1. – С. 92-95.
10. Никонов В.И. Повышение информационной безопасности при передаче данных // Материалы VII международной научно технической конференции «Динамика систем, механизмов и машин» 10-12 ноября 2009. – Омск: издательство ОмГТУ, 2009. - С.321-325

11. Никонов В.И. Применение корреляционных кодов для систем синхронизации и связи / В.И. Никонов, Г.С. Никонова // Техника радиосвязи. Научно-технический сборник. – Омск: издательство Омского научно-исследовательского института приборостроения.- Выпуск 13. – С.87-90.
12. Никонов В.И. Маршрутизируемый сервис передачи // Приложение к научному журналу «Прикладная дискретная математика»: тезисы докладов VIII Сибирской школы-семинара с международным участием «Компьютерная безопасность и криптография» - SIBECRYT'09 (Омск, ОмГТУ, 8-11 сентября 2009г.). – Томск: Томский государственный университет.– №1. – С. 76-78.
13. Никонов В.И. Маршрутизируемый сервис передачи данных повышенной информационной безопасности // Материалы региональной научно-практической конференции «Наука, образование, бизнес». – Омск: институт радиоэлектроники, сервиса и диагностики, 2009. – С. 136-137.
14. Никонов В.И. Атаки на маршрутизируемый трафик // Информационные технологии моделирования и управления. Научно-технический журнал. – Воронеж: издательство «Научная книга», 2009. – №7(59). – С. 962-968.
15. Никонов В.И. Передача данных через распределенные сети // Тезисы докладов региональной молодежной научно-технической конференции «Омское время – взгляд в будущее» 14-15 апреля 2010 г.- Омск: издательство ОмГТУ, 2010. – Книга 1. – С.157-158.