УДК 004.738.5

Маскирование интегрированных сетей связи ведомственного назначения

Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В.

Постановка задачи: *в условиях развития информационных технологий, интеграции сетей связи ведомственного назначения и общего пользования необходимы меры по защите интегрированных сетей связи ведомственного назначения от компьютерной разведки, реализуемые с целью формирования у злоумышленников ложного представления о структуре ведомственной системы управления посредством управления демаскирующими признаками информационного обмена. Такая цель может быть достигнута реализацией маскирующего обмена. Однако, в связи с недостаточным развитием методического и технологического обеспечения для его реализации при использовании сетей связи общего пользовании в настоящее время задача скрытия факта передачи конструктивного трафика и искажения уровней иерархии узлов связи соответствующих органов управления (подразделений) в интегрированных сетях связи ведомственного назначения не решена.* ***Целью работы*** *является разработка математической модели синтеза структуры сети маскирующего обмена и методики реализации маскирующего обмена для повышения защищенности интегрированных сетей связи ведомственного назначения от компьютерной разведки.* ***Используемые методы****: решение задачи маскирования интегрированных сетей связи ведомственного назначения основано на использовании теории графов в части построения минимальных остовных деревьев по критерию минимальной интенсивности информационного обмена между узлами сети, а также дифференциации маршрутов между узлами связи по критерию безопасности транзитных узлов связи.* ***Научная новизна*** *разработанного научно-методического аппарата заключается в модификации алгоритмов минимальных остовных деревьев, их применении для решения задачи синтеза структуры сети маскирующего обмена и реализации маскирующего обмена при дифференциации маршрутов между узлами связи по критерию безопасности транзитных узлов связи.* ***Практическая значимость*** *разработанного научно-методического аппарата заключается в обеспечении возможности искажения алгоритмов функционирования интегрированных сетей связи ведомственного назначения при защите от компьютерной разведки по заданным требованиям (в соответствии с замыслом обмана), снижении нагрузки абонентов сети обработкой маскирующих сообщений и обеспечении своевременности доставки сообщений при осуществлении маскирующего обмена.* ***Результат****: использование разработанного научно-методического аппарата позволяет реализовать маскирующий обмен для выполнения замысла обмана при уменьшении нагрузки на абонентов сети обработкой маскирующих сообщений и обеспечении своевременности доставки сообщений. Проведенное имитационное моделирование для сети из 9 узлов показывает, что время передачи 1 Мбит конструктивного трафика при вводе узлов-терминаторов уменьшается в среднем на 25 % от реализации маскирующего обмена без них.*

Ключевые слова: *демаскирующие признаки, сеть связи, маскирующий обмен, минимальное остовное дерево, узел-терминатор.*

Библиографическая ссылка на статью:
Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136-175. URL: http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf.

Reference for citation:
Sherstobitov R. S., Sharifullin S. R., Maximov R. V. Masking of departmental-purpose integrated communication networks. *Systems of Control, Communication and Security*, 2018, no. 4, pp. 136-175. Available at: http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf (in Russian).

Введение

Современный этап развития информационных технологий характеризуется интеграцией сетей связи ведомственного назначения и сетей связи общего пользования (ССОП). Следовательно, у злоумышленников, также имеющих доступ к ССОП, существует возможность вести компьютерную разведку с целью получения сведений о закономерностях функционирования интегрированных сетей связи ведомственного назначения (ИСС ВН) для осуществления хорошо спланированных и целенаправленных деструктивных воздействий и нарушения функционирования системы управления ведомства. Одним из основных общих свойств современных технологий является их критическая зависимость друг от друга [1, 2]: путем взаимопроникновения и поглощения происходит интеграция процессов электросвязи, устройств, сетей и служб, и инфокоммуникационные услуги перестают быть связанными с определенными видами сетей, так как благодаря цифровизации сетей и абонентских терминалов стало возможным передавать любую информацию по любой цифровой сети [3, 4]. В настоящий момент потребности в передачи всех видов информации между подразделениями ведомства обеспечивается универсальной транспортной сетью. Такой универсальной транспортной сетью являются ССОП.

В таких условиях необходимы меры по защите ИСС ВН от компьютерной разведки, реализуемые с целью формирования у злоумышленников ложного представления о структуре ведомственной системы управления посредством управления демаскирующими признаками (ДМП) информационного обмена. Такая цель может быть достигнута реализацией маскирующего обмена.

В рамках статьи под ИСС ВН будем понимать сеть связи, состоящую из совокупности территориально удаленных узлов и линий связи объединенных посредством ССОП для выполнения задач по обеспечению информационного обмена в ведомственной системе управления.

Интеграция сетей связи ВН и ССОП не позволяет при их защите использовать традиционную концепцию контролируемых зон, а также корректно определять границу внешней среды объекта защиты, так как транзитные узлы связи (УС) принадлежат сторонним организациям (различным операторам связи) [5-7]. Кроме того, инфраструктура ССОП выполнена с высокой долей импортной электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи [8], что создает угрозу использования злоумышленником недекларированных возможностей, встраиваемых на уровне программного или аппаратного обеспечения.

Данные факты дают возможность вести компьютерную разведку с целью получения сведений о закономерностях функционирования ИСС ВН для планирования целенаправленных деструктивных воздействий и нарушения функционирования ведомственной системы управления, в интересах которой и строят ИСС ВН [9].

В связи с этим, Министерство связи РФ в 2017 году начало разработку проекта закона «Об интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка» на основе положений

Доктрины информационной безопасности и в соответствии со стратегией национальной безопасности России. Целями разработки проекта закона является:

- правовое регулирование создания и эксплуатации интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка;
- создание условий для оказания услуг интегрированной сети связи для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка на всей территории Российской Федерации;
- создание условий для обеспечения функционирования интегрированной сети связи;
- обеспечение централизованного управления интегрированной сетью связи для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка;
- установление требований к лицам и осуществлению деятельности в области создания, управления, эксплуатации и развития интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка;
- установление требований к средствам и линиям интегрированной сети связи и ресурсу сети электросвязи, используемым для функционирования интегрированной сети связи.

Законопроектом предполагалось создание отдельной сети связи для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка. Такая сеть должна быть изолирована от ССОП и представлять собой выделенную структуру для госорганов и спецслужб, не имеющую соединений с сетями общего доступа. Для ее построения планировалось использовать доверенное оборудование, аппаратно-программные средства и программное обеспечение. Однако, высокая стоимость построения такой сети связи, а также противоречия как концептуального, так юридического и технического характеров привели к тому, что до настоящего времени закон не принят.

Невозможность и нецелесообразность физически выделить инфраструктуру управления ведомствами в масштабах страны и, как следствие, использование ССОП при ее построении порождает противоречие между необходимостью выполнения специфических требований к управлению территориально распределенными подразделениями и недостаточным развитием методического и технологического обеспечения для их реализации при использовании ССОП. Например, это выражается в том, что необходимо скрывать факт передачи конструктивного трафика и искажать уровни иерархии узлов связи соответствующих органов управления (подразделений) в ИСС ВН. Однако, ограниченные ресурсы и адаптационные возможности маршрутов связи для передачи конструктивного и маскирующего трафика, а также отсутствие научно-методического аппарата выбора структуры сети маскирующего обмена и количественных значений показателей интенсивности маскирующего трафика препятствуют реализации данных задач.

Здесь и далее под маскирующим обменом следует понимать упорядоченную по структуре и интенсивности совокупность ложных пакетов сообщений, формируемых корреспондентами ИСС ВН с целью управления ДМП алгоритмов функционирования скрываемой системы управления, увеличивающих видимую интенсивность информационного обмена между пунктами управления. Идентифицировать в ССОП объект разведки и исследовать закономерности его функционирования злоумышленник может из-за наличия ДМП элементов ИСС ВН. Под ДМП объекта (системы, средства) понимают [10, 11] характеристику физического поля (качественную, количественную), которая создается (отражается, искажается) объектом защиты, если эта характеристика раскрывает наличие объекта (отличие его от других). ДМП присущи каждому объекту защиты. Именно наличие ДМП элементов ИСС ВН позволяет нарушителю решать свои задачи по идентификации объектов для целенаправленных компьютерных атак. В свою очередь, система защиты должна иметь механизмы целенаправленного управления ДМП с целью создания искаженных образов объектов компьютерной разведки и достижения замысла введения нарушителя в заблуждение. В [1, 2, 12] авторами проведена содержательная декомпозиция ДМП ИСС ВН по структуре, составу и алгоритмам функционирования (рис. 1).

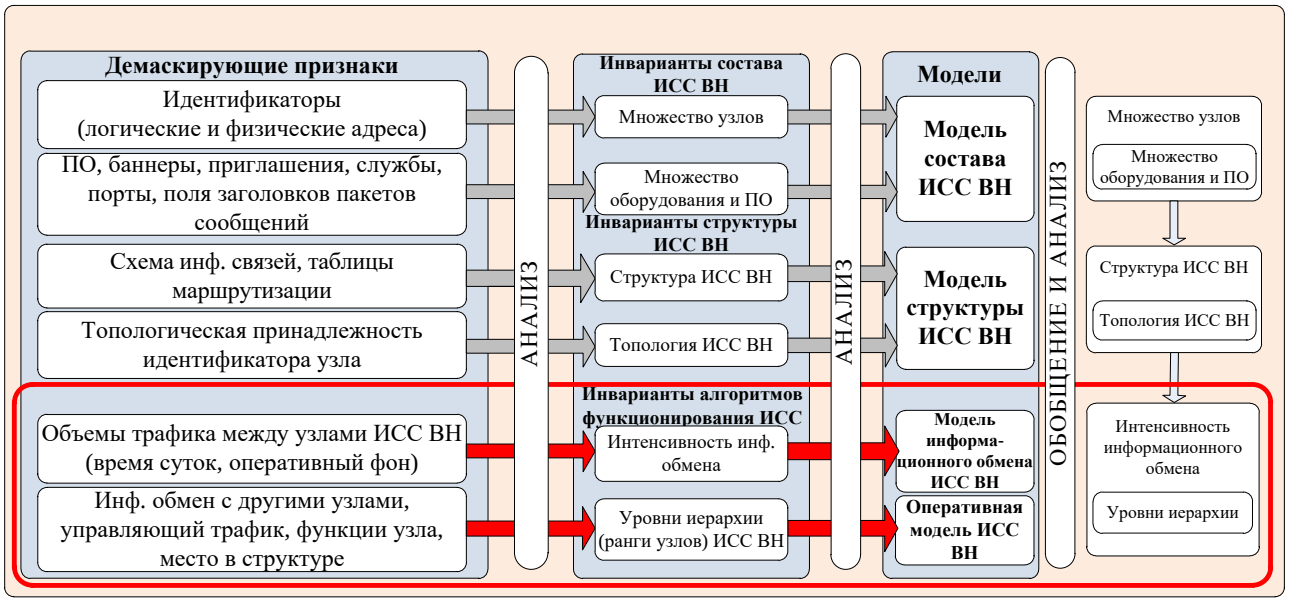

Рис. 1. Демаскирующие признаки ИСС ВН

Область исследования авторов статьи лежит в нижней трети схемы – ДМП алгоритмов функционирования ИСС ВН. Именно алгоритмы функционирования скрывают (искажают) посредством реализации маскирующего обмена. Наиболее информативными ДМП алгоритмов функционирования являются:

- интенсивность (объемы) трафика между УС пунктов управления (ПУ);
- связность информационного обмена между УС ПУ.

Доступность алгоритмов функционирования ИСС ВН обуславливается низкой скрытностью при передаче трафика между абонентами сети, использующими открытые IP-адреса, и возможностью идентификации по ним пакетов

сообщений относительно конкретных пользователей сети и (или) УС (далее – сетевых информационных объектов, СИО). Например, использование абонентами для подключения к ССОП одного маршрутизатора демаскирует их принадлежность к одному УС (СИО). В подобных случаях считают, что нарушитель реконструирует (вскрывает) структуру ИСС ВН и может осуществлять деструктивные воздействия на ее элементы, а сами алгоритмы функционирования ИСС ВН обладают низкой скрытностью [13-15]. Таким образом, реконструкция алгоритмов функционирования ИСС ВН происходит вследствие известности (открытости) структуры пакетов сообщений, где адреса отправителя и получателя демаскируют абонентов сети.

Математическая модель синтеза структуры сети маскирующего обмена в ИСС ВН

Целями разработки математической модели является:

- выбор критериальной оценочной базы результативности и эффективности маскирующего обмена;
- выбор математического аппарата, позволяющего верифицировать результативность и эффективность маскирующего обмена;
- разработка алгоритмов, позволяющих получать обоснованные решения в рамках выбранного математического аппарата;
- обоснование направлений, путей и способов создания методики и научно-технических предложений по реализации маскирующего обмена.

Результативность маскирующего обмена достигается увеличением объема трафика между узлами ИСС ВН и формированием маскирующих (ложных) связей между УС ПУ для искажения уровней их иерархии [16, 17], а также автоматизацией полученных решений. Для того, чтобы исказить ДМП алгоритмов функционирования ИСС ВН необходимо в качестве исходных данных принять требуемую ложную структуру ведомственной системы управления, имитировать которую требуется. Навязывание злоумышленнику такой структуры вынудит его принимать решения в условиях неполноты и противоречивости информации, и некорректно определять первоочередные цели для информационно-технических воздействий (компьютерных атак) [18-20]. Степень близости сформированной структуры ИСС к ложной структуре ведомственной СУ и определяет, в конечном итоге, результативность маскирующего обмена. Автоматизация полученных решений достигается тем, что суммарную интенсивность трафика информационного направления задают как степень его утилизации конструктивным и маскирующим трафиком. При увеличении (уменьшении) конструктивного трафика – маскирующий пропорционально уменьшают (увеличивают).

Пусть, например, здесь и далее дополнительные ложные УС в структуру ИСС ВН не вводятся, а искажаются ранги существующих УС (в частности – инверсией их важности). Тогда показателем, характеризующим результативность маскирующего обмена (достижения целей имитации) будет являться сходство имитируемых (навязываемых злоумышленнику) ложных структур ве-

домственной СУ и ИСС ВН, а в пределе – их биекцией (взаимно однозначным отображением). В связи с тем, что структура СУ содержит значительно больше элементов, чем структура ИСС, целесообразно использовать коэффициент сходства. Пусть $P(K_{СХ} \geq K_{СХ}^{Треб})$ – вероятность того, что выполняется условие $K_{СХ} \geq K_{СХ}^{Треб}$, характеризующие подобие структуры ИСС ВН структуре ложной СУ. Вскрывая с высокой полнотой структуру ИСС средствами компьютерной разведки, злоумышленник вскрывает ложную структуру СУ, чем и достигается его дезинформация [21-23]. С учетом того, что структурная связность элементов ИСС и их количество являются регулируемыми системой защиты параметрами, качество вскрытия злоумышленником ложной структуры можно представить следующим выражением:

$$P_{Вскр}^{ИСС} = P_{КР}^{S} P(K_{СХ} \geq K_{СХ}^{Треб}), \quad (1)$$

где $P_{КР}^{S}$ – характеристика полноты добытых разведданных (в наиболее жестких для системы защиты условиях $P_{КР}^{S} \to 1$, следовательно $P_{Вскр}^{ИСС} \approx P(K_{СХ} \geq K_{СХ}^{Треб})$), $s = 1..S$ – структурные элементы ИСС, характеризующиеся ценностью для злоумышленника и взаимной связностью.

С другой стороны, критерием оценки полученной ложной ИСС может служить степень отличия от реальной структуры. Если обратиться к теории обфускации, которая в настоящее время применяется в области программирования (в буквальном переводе означает скрывать, запутывать), то такой критерий можно определить как степень обфускации структуры ИСС [24, 25]. Однако для использования этого критерия необходим некий ассортимент ложных структур для их сравнительной оценки. В настоящей статье задача синтеза в такой постановке не ставится, так как предполагается требуемую ложную структуру СУ принимать в качестве исходных данных для ее реализации структурой ложной ИСС.

Эффективность маскирующего обмена достигается снижением эксплуатационных и ресурсных затрат на маскирующий обмен, качеством информационного обеспечения и оптимальностью управления процессами защиты. Известно, что любая защита достигается тем, что на нее затрачивают некий (защитный) ресурс. ИСС предназначены для конструктивного информационного обмена, следовательно, маскирующий трафик, используя совместно с конструктивным неделимый ресурс каналов связи и средств обработки информации сетевых информационных объектов (СИО), создает дополнительную нагрузку на них. Эффективный маскирующий обмен – это, прежде всего, необходимый и достаточный маскирующий обмен, позволяющий достичь требуемой для навязывания контрастности элемента структуры (по сравнению с конкурирующими элементами) и относительной частоты появления связей между ложными элементами (для обеспечения искажения структуры в целом). Эффективность может достигаться снижением ограничений на производительность СИО и пропускную способность каналов связи, и обеспечением своевременности информационного обмена. При этом производительность СИО и пропускная способность каналов связи выступают в качестве очевидных ограничений,

а своевременность информационного обмена $K_{\text{ИО}}$ определяют [26] через показатели своевременности обработки $K_{\text{Обр}}$ и своевременности доставки $K_{\text{Д}}$ следующими соотношениями:

$$K_{\text{Обр}} = P(T_{\text{Обр}} \le T_{\text{Обр}}^{\text{Доп}}), \quad (2)$$

$$K_{\text{Д}} = P(T_{\text{Д}} \le T_{\text{Д}}^{\text{Доп}}), \quad (3)$$

$$K_{\text{ИО}} = K_{\text{Д}} \cdot K_{\text{Обр}}. \quad (4)$$

Время обработки $T_{\text{Обр}}$ и время доставки $T_{\text{Д}}$ являются контекстно зависимыми величинами, то есть требуют достаточно точно определять состав канала (каналов) связи, конкретизировать функции СИО и процессов обработки (доставки) относительно уровней ЭМВОС. Так, например, процессы фрагментации (дефрагментации) пакетов сообщений могут осуществляться не только у конечных абонентов, но и на транзитных УС, и не связаны с содержательной обработкой информации [27].

В данном случае наиболее удобным показателем, характеризующим эффективность маскирующего обмена будет являться среднее время информационного обмена $\overline{T}_{\text{ИО}}$ одной единицей (например, 1 Мбит) конструктивного трафика или обратный ему – средняя скорость информационного обмена $\overline{V}_{\text{ИО}}$ в единицу времени (Мбит/с).

Маскирующий трафик передают в канал связи только во время отсутствия конструктивного, причем ограничивают его объем так, чтобы реализовать именно требуемые ложные ранги СИО. Снижение значения $\overline{T}_{\text{ИО}}$ у передающего корреспондента достигают уменьшением длины пакетов маскирующих сообщений, что приводит к уменьшению среднего времени нахождения пакетов конструктивных сообщений в очереди на передачу. Снижения значения $\overline{T}_{\text{ИО}}$ у принимающего корреспондента достичь использованием известных подходов нельзя, так как очереди у принимающего СИО создают пакеты сообщений, поступивших на обработку от разных источников. Следует разработать новые алгоритмы, методику и реализующие их технические решения.

Используя известный математический аппарат жадных алгоритмов, необходимо построить на структуре ИСС минимальное остовное дерево для сети маскирующего обмена, и модифицировать полученную оптимальную структуру до возможности получения приемлемых структур ИСС, где выполняется условие $K_{\text{СХ}} \ge K_{\text{СХ}}^{\text{Треб}}$.

Обоснование направлений, путей и способов создания методики и научно-технических предложений по реализации маскирующего обмена включает в себя исследование технологических возможностей ИСС ВН для реализации маскирующего обмена в условиях ограничения ресурсов связи, выбор комбинации наилучших способов маскирования, поддерживаемых ССОП и синтез новых технических решений.

Рассмотрим общую содержательную постановку задачи обеспечения результативности маскирующего обмена. Каждый узел ИСС ВН имеет некоторую важность (ранг), отражающую его принадлежность определенному звену

управления. Стратегия злоумышленника – распределить ограниченный неоднородный ресурс средств разведки и подавления так, чтобы выявить и подавить наиболее важные узлы ИСС ВН. Наилучшая стратегия защиты – распределить ограниченный неоднородный ресурс средств защиты по взаимосвязанным элементам ИСС ВН так, чтобы сформировать ложную структуру ИСС ВН [28, 29]. Общий алгоритм достижения результативности маскирующего обмена включает в себя следующие действия:

- построить взвешенный связный неориентированный граф, отражающий функционально-логическую структуру ИСС ВН;
- выбрать (назначить) УС или информационное направление (ложные), замещающие соответствующие элементы высшего ранга в исходной структуре;
- решить задачу построения структуры сети маскирующего обмена поиском минимального остовного дерева;
- в соответствии с замыслом обмана преобразовать найденное минимальное остовное дерево в искомую структуру ИСС ВН, где выполняется условие $K_{\text{СХ}} \geq K_{\text{СХ}}^{\text{Треб}}$;
- рассчитать требуемую нагрузку маскирующего трафика для полученной структуры сети маскирующего обмена.

Рассмотрим математическую постановку задачи обеспечения результативности маскирующего обмена.

Пусть $G = (V, E)$ – связный неориентированный граф, где V – множество узлов, E – множество ребер. Для каждого ребра $(u, v) \in E$ задан вес $w(u, v)$, определяющий интенсивность трафика между u и v.

Необходимо найти ациклическое подмножество $T \subset E$, которое соединяет все вершины и общий вес которого $\omega(T) = \sum_{(u,v)\in T} \omega(u,v) \to \min$, то есть его минимальное остовное дерево. Далее последовательно добавлять ребра $(u, v) \in E$ для получения искомой ($K_{\text{СХ}} \geq K_{\text{СХ}}^{\text{Треб}}$) маскирующей структуры T^M, одновременно удаляя конкурирующие ребра из подмножества T. Рассчитать требуемую нагрузку маскирующего трафика для T^M такую, что

$$\omega(T^M) = \sum_{(u,v)\in T^M} \omega^{\text{Треб}}(u,v).$$

Для построения минимального остовного дерева $T \subset E$ используют алгоритмы Краскала (при построении от минимального информационного направления) и Прима (при построении от назначенного ложного УС). В связи с тем, что построенная структура не будет отражать замысел обмана, а будет являться минимальным T-подграфом заданного графа, далее необходимо последовательно добавлять ребра в этот подграф, которые будут приближать структуру T к структуре T^M до выполнения условия $K_{\text{СХ}} \geq K_{\text{СХ}}^{\text{Треб}}$ в соответствии с замыслом введения в заблуждение и удалять конкурирующие ребра, образующие петли.

Рассчитывать требуемую нагрузку маскирующего трафика на полученной структуре необходимо осуществлять по формуле:

$$\omega((u,v) \in T^M) = \omega(u,v)_S - \omega(u,v)_{T^M} + \omega(u,v)_S, \quad (5)$$

где $\omega(u,v)_S$ – интенсивность замещаемого (S – от англ. substitution, замещение) ИН.

Рассмотрим, например, использования разработанной математической модели для решения расчетной задачи синтеза структуры сети маскирующего обмена.

Пусть исходными данными для примера расчета по разработанной модели синтеза структуры сети маскирующего обмена является вариант исходной структуры ИСС. На рис. 2 представлена легенда, иллюстрирующая ассортимент иерархий УС, и ее графовая интерпретация. Узлом связи высшего ранга в представленной структуре является УС № 1.

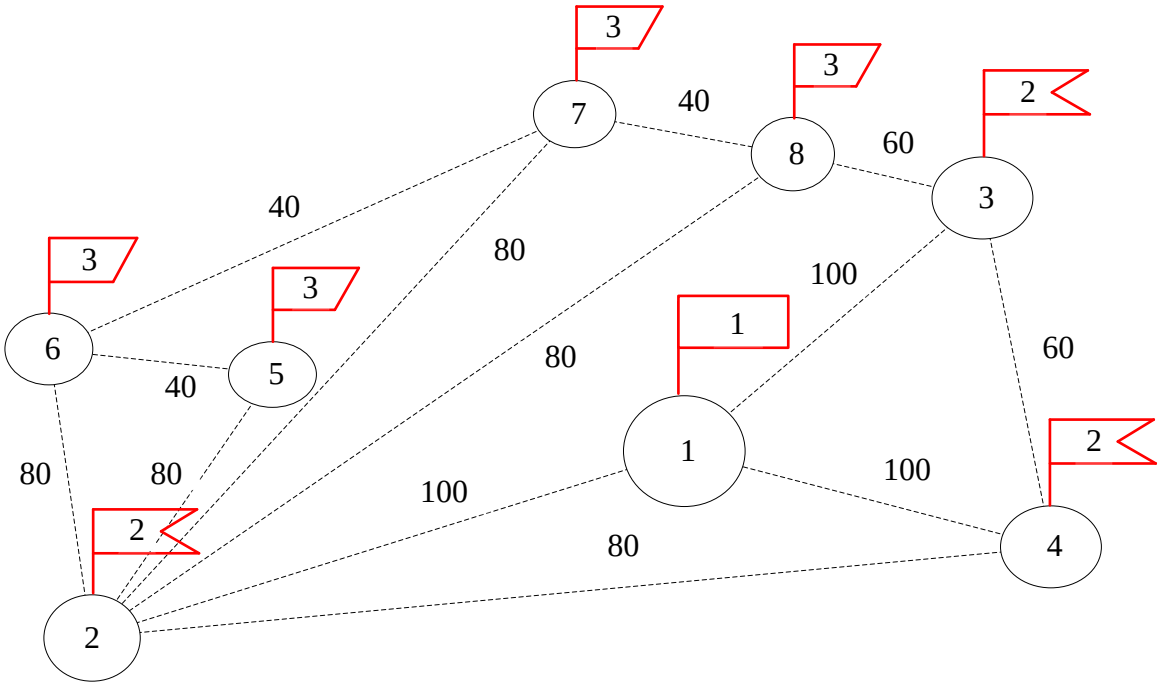

Рис. 2. Вариант исходной структуры ИСС ВН

В соответствии с замыслом введения в заблуждение выбираем (назначаем) в качестве ложного УС высшего ранга УС № 7.

В соответствии с алгоритмом Прима находим минимальное остовное дерево (сплошные ребра на рис. 3) на структуре ИСС ВН, в котором вес ребер $\omega(T) = \sum_{(u,v)\in T} \omega(u,v) \to \min$. После построения минимального остовного дерева ИСС ВН, добавляя недостающие ребра и удаляя конкурирующие, найдем необходимую, в соответствии с замыслом введения в заблуждение, структуру сети маскирующего обмена T^M (рис. 4).

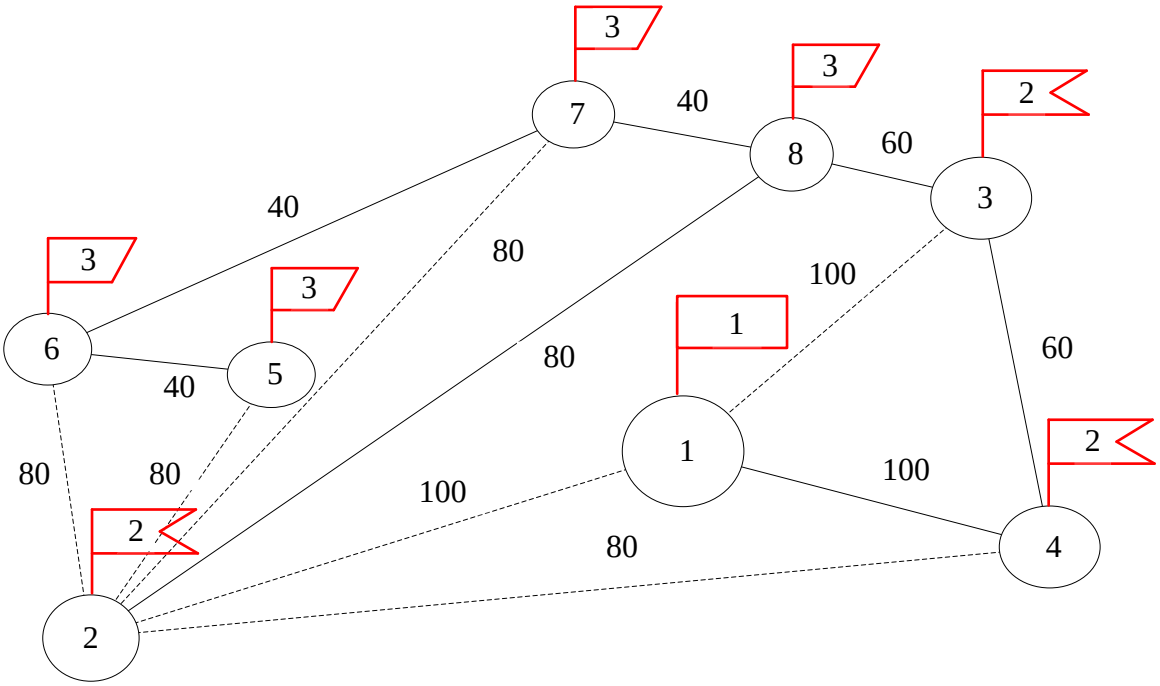

Рис. 3. Построение минимального остовного дерева по алгоритму Прима

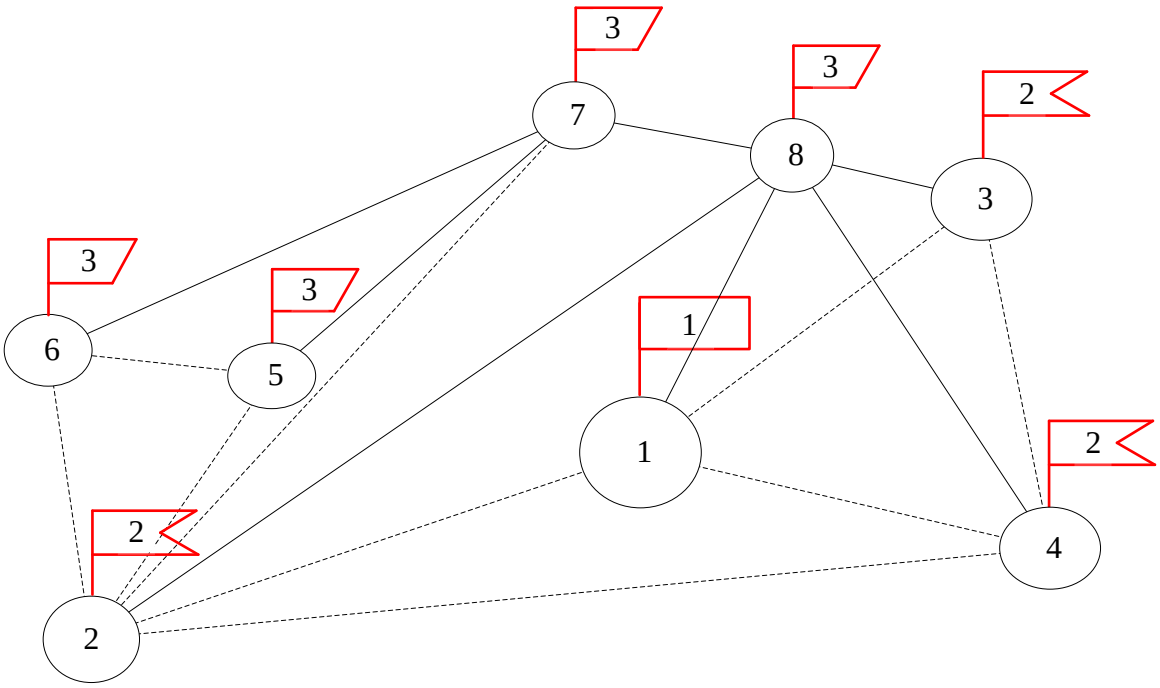

Рис. 4. Структура сети маскирующего обмена в ИСС ВН

Далее необходимо рассчитать маскирующую нагрузку для искажения алгоритмов функционирования ИСС ВН.

Введем определения замещаемого УС, замещающего УС, замещаемого ИН, замещающего ИН.

Замещаемый УС – УС, ранг которого необходимо исказить (снизить) маскирующим обменом.

Замещающий УС – УС, ранг которого необходимо исказить (повысить) маскирующим обменом в соответствии с замыслом введения в заблуждение.

Замещаемое ИН – информационное направление между двумя узлами связи, интенсивность информационного обмена которого необходимо исказить (снизить) маскирующим обменом.

Замещающее ИН – информационное направление, ранг которого необходимо исказить (повысить) маскирующим обменом в соответствии с замыслом введения в заблуждение.

Пример построения сети маскирующего обмена и расчет интенсивности маскирующего трафика информационных направлений представлен в таблице 1, где приняты следующие аббревиатуры: ИН – информационное направление, КТ – конструктивный трафик, МТ – маскирующий трафик.

Таблица 1 – Пример построения сети маскирующего обмена и расчета интенсивности маскирующего трафика информационных направлений

ИН в ИСС	Интенсивность КТ в ИН	Значение ИН при преобразованию к T^M	Функция в T^M	Формула расчета интенсивности маскирующего трафика по ИН	Интенсивность ИО (КТ + МТ)
w_{12}	100	Замещаемая на w_{67}	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	100
w_{13}	100	Замещаемая на w_{57}	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	100
w_{14}	100	Замещаемая на w_{78}	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	100
w_{24}	80	Неизменно	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	80
w_{25}	80	Замещаемая на w_{18}	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	80
w_{26}	80	Замещаемая на w_{38}	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	80
w_{27}	80	Замещаемая на w_{48}	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	80
w_{34}	60	Неизменно	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	60
w_{56}	40	Неизменно	Только КТ	ИН не входит в структуру сети маскирующего обмена T^M	40
w_{28}	80	Замещающая w_{14}	КТ и МТ	$w^M_{28} = w_{14} - w_{28} + w_{14} = 100 - 80 + 100$	120
w_{38}	60	Замещающая w_{26}	КТ и МТ	$w^M_{38} = w_{26} - w_{38} + w_{26} = 80 - 60 + 80$	100
w_{67}	40	Замещающая w_{12}	КТ и МТ	$w^M_{67} = w_{12} - w_{67} + w_{12} = 100 - 40 + 100$	160
w_{78}	40	Замещающая w_{14}	КТ и МТ	$w^M_{78} = w_{14} - w_{78} + w_{14} = 100 - 40 + 100$	160
w_{18}	-	Замещающая w_{25}	Только МТ	$w^M_{18} = w_{25} - w_{18} + w_{25} = 80 - 0 + 80$	160
w_{48}	-	Замещающая w_{27}	Только МТ	$w^M_{48} = w_{27} - w_{48} + w_{27} = 80 - 0 + 80$	160
w_{57}	-	Замещающая w_{13}	Только МТ	$w^M_{57} = w_{13} - w_{57} + w_{13} = 100 - 0 + 100$	200

Информационные направления w_{18}, w_{48}, w_{57} отсутствуют в исходной структуре и предназначены для передачи только маскирующего трафика.

При таком способе расчета маскирующей нагрузки неизбежны следующие ограничения. Если замещаемое ИН совпадает с замещающим (см. w_{28} в табл. 1), то интенсивность либо не меняется, либо такое ИН замещает произвольно выбранное ИН исходной структуры (в табл. 1 w_{28} замещает w_{14}). Так как маскирующий трафик не может иметь отрицательное значение (т. е. снизить интенсивность конструктивного трафика), то нет решения по замещению ИН с большей интенсивностью.

Результаты расчета интенсивности маскирующего трафика для построенной структуры сети маскирующего обмена T^M графически представлены на рис. 5.

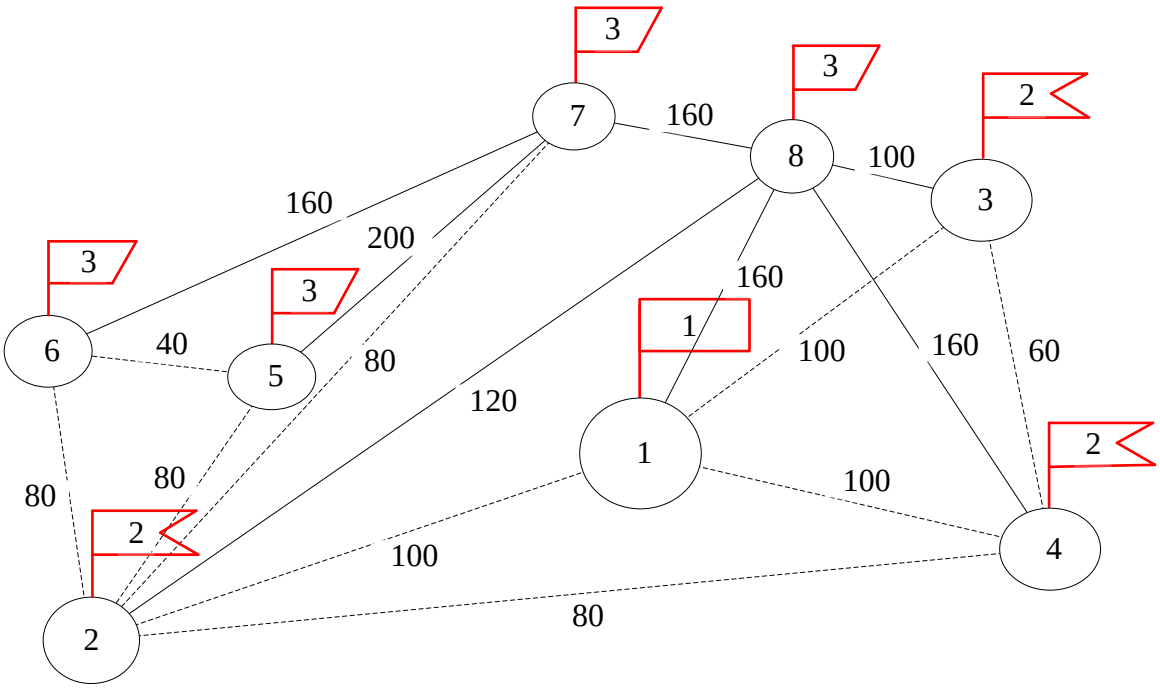

Рис. 5. Результаты расчета интенсивности маскирующего трафика

Тогда результатом построения сети маскирующего обмена в ИСС ВН станет ложная функционально-логическая структура, представленная на рис. 6.

Научная новизна разработанной модели заключается в модификации алгоритмов минимальных остовных деревьев и их применении для решения задачи синтеза структуры сети маскирующего обмена.

Практическая значимость разработанной модели заключается в обеспечении возможности искажения алгоритмов функционирования ИСС ВН по заданным требованиям (в соответствии с замыслом обмана).

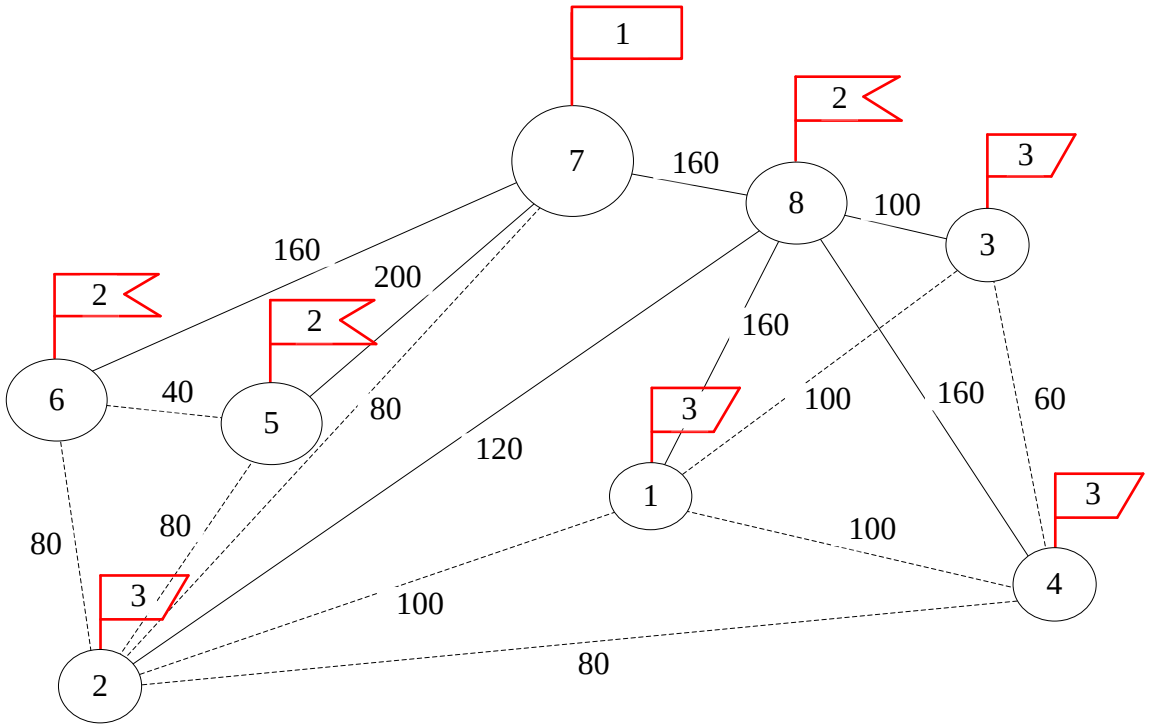

Рис. 6. Полученная ложная ФЛС ИСС ВН

Методика реализации маскирующего обмена в ИСС ВН

Разработанная математическая модель синтеза структуры сети маскирующего обмена не учитывает ограниченные ресурсы и параметры безопасности маршрутов связи при передаче конструктивного и маскирующего информационного трафика через ССОП.

В результате анализа способов реализации маскирующего обмена в рамках эталонной модели взаимодействия открытых систем выявлены следующие технические особенности ССОП.

Во-первых, у передающего абонента (СИО) возникают очереди из пакетов конструктивных сообщений, так как СИО занят формированием пакетов маскирующих сообщений.

Во-вторых, у принимающего абонента (СИО) возникают очереди из пакетов конструктивных и маскирующих сообщений, так на вход принимающего СИО могут одновременно прийти пакеты сообщений от нескольких отправителей. В результате ухудшаются значения показателей своевременности доставки сообщений, а услуги связи, критичные к выполнению требований по своевременности доставки сообщений, могут стать субъективно «некачественными» – ухудшится разборчивость речи, качество видеоизображения и т. д.

Назначение методики – решение задачи маскирования алгоритмов функционирования ИСС ВН при снижении маскирующей нагрузки на абонентов сети и обеспечении своевременности доставки пакетов конструктивных сообщений.

Решить данную задачу можно использованием технологических возможностей ИСС ВН для реализации маскирующего обмена в условиях ограничения ресурсов связи и комбинацией способов маскирования, потенциально поддерживаемых ССОП.

В настоящее время теоретической и практической возможностью для реализации маскирующего обмена является только установка для корреспондентов меток, означающих, что данный конкретный пакет сообщений является маскирующим или содержит полезную информацию [30]. При этом предполагается, что маскирующий пакет сообщений будет игнорироваться принимающим СИО, но, тем не менее, он будет создавать нагрузку на его входе. Единственным достоинством данного решения является то, что установка меток, а также фрагментация пакетов маскирующих сообщений осуществляется без дополнительных технических решений.

Анализ протоколов ССОП позволил вскрыть следующие пути управления маскирующей нагрузкой.

Во-первых, в процессе формирования пакетов сообщений на передачу можно устанавливать значения полей пакетов сообщений TTL (Time To Live) и Hop Limit такими, чтобы пакеты сообщений не доходили до приемника и пакет терминировался в заведомо выбранном СИО ССОП. В качестве такого СИО целесообразно выбрать последний (в маршруте) СИО (маршрутизатор) ССОП. Между ним и СИО ИСС ВН наличие средств КР злоумышленника наименее вероятно по той причине, что злоумышленник решает ресурсную задачу, а размещение средств КР в каждой точке распределенной ИСС ВН будет неоптимальным и может скомпрометировать систему разведки. Однако, у данного способа есть очевидные недостатки:

- наличие прямого ДМП в заголовке – злоумышленник при длительном наблюдении может определить регулярность некорректных значений TTL (Hop Limit) и скомпрометировать маскирующий трафик;
- наличие косвенного ДМП – узел, на котором прекращается дальнейшая передача пакета, информирует узел-отправитель ICMP-сообщением (с учетом предустановленного лимита на количество ICMP-сообщений) о невозможности доставить пакет адресату;
- отсутствие гарантированного уничтожения пакета в выбранной точке ССОП из-за наличия альтернативных более коротких маршрутов.

Во-вторых, технологической возможностью для реализации маскирующего обмена является построение карты сети со значениями MTU каждого узла сети, принадлежащего маскирующему маршруту по процедуре Path MTU Discovery [31] и обоснованным выбором значений MTU маскирующих пакетов сообщений таких, чтобы пакеты сообщений не доходили до приемника и терминировались в заведомо выбранном СИО ССОП. Данный способ также не лишен недостатков:

- наличие прямого ДМП в заголовке IPv4;
- наличие косвенного ДМП – при невозможности фрагментации пакетов сообщений на транзитных узлах (для прекращения ретрансляции пакета сообщений в подсеть с меньшим значением MTU необходима установка флага Do Not Fragment (DF)), транзитный узел ССОП отправляет узлу-отправителю управляющее ICMP-сообщение (с учетом предустановленного лимита на количество ICMP-сообщений) о невозможности доставить пакет адресату;

- при предустановленной блокировке ответов по протоколу ICMP выполнение процедуры Path MTU Discovery невозможно, и данная ситуация получила название MTU Discovery Black Hole.

В-третьих, технологической возможностью для реализации маскирующего обмена является согласование с приемником значения TCP Maximum segment size (MSS) для маскирующего трафика и обоснованный выбор таких значений MTU маскирующего пакета сообщений, чтобы пакеты сообщений не доходили до приемника и пакеты терминировались на предпоследнем транзитном СИО ССОП. Данный способ также имеет недостаток: наличие косвенного ДМП – при невозможности фрагментации пакетов сообщений на транзитных узлах (при установке флага Do Not Fragment (DF)) транзитный узел ССОП отправляет узлу-отправителю управляющее ICMP-сообщение (с учетом предустановленного лимита на количество ICMP-сообщений) о невозможности доставить пакет адресату.

Рассмотренные три способа исключают нагрузку на СИО принимающего абонента и открыты для создания новых технических решений, расширяющих ассортимент средств СИО ИСС ВН, а их комбинированное использование при организации маскирующего обмена позволит снизить информативность присущих им ДМП.

Итак, для обоснования выбора значений TTL (Hop Limit), MTU и TCP MSS необходимо использованием процедуры Path MTU Discovery построить карту ССОП с указанием значений MTU узлов сети, принадлежащих маскирующему маршруту. После этого выбрать узел-терминатор маскирующих сообщений, который прекращает дальнейшую передачу пакетов, если длина пакета больше принятого на узле-терминаторе значения MTU.

Значение MTU маскирующего пакета сообщений должно быть большим, чем значение MTU узла-терминатора. В том случае, если выбираемое минимальное значение MTU не позволит терминировать пакет в заданном СИО ССОП, необходимо дополнительно провести согласование между корреспондентами значения TCP MSS и задавать его значение у передающего корреспондента больше на некоторую (переменную) величину (от 1 байта).

Имеющиеся на рынке средства создания VPN-туннелей (такие как, например, линейка средств DioNIS, программно-аппаратные комплексы «Атликс-VPN», «Застава», «Континент» и другие) имеют технические возможности реализовывать протокольно указанные процедуры для осуществления маскирующего обмена.

Физическая (содержательная) постановка задачи.

Информационный обмен между абонентами ИСС ВН осуществляют маршрутизацией пакетов сообщений через последовательность транзитных узлов ССОП. Совокупность перечисленных элементов систем образует ИСС ВН.

Наиболее уязвимым местом ИСС ВН является их функционально-логическая структура, вскрытие которой приводит к компрометации структуры системы управления (СУ) ведомства [1, 2]. Реконструкция структуры ИСС, и, как следствие, алгоритмов функционирования, происходит вследствие извест-

ности (открытости) структуры пакетов сообщений, где адреса отправителя и получателя демаскируют абонентов сети.

Для реализации маскирующего обмена в ИСС ВН необходимо:

- применить математическую модель синтеза структуры сети маскирующего обмена, задать замещающий УС высшего уровня иерархии, как точку истока маскирующего трафика в T^M, и замещающие информационные направления между узлами связи;
- построить схему (граф) совокупности альтернативных маршрутов связи между каждой парой абонентов УС ПУ $(u, v) \in T^M$, содержащую транзитные узлы ССОП;
- сформировать совокупность допустимых $N_{ij}^{\text{доп}}$ маршрутов для передачи по ним конструктивных сообщений между каждой парой абонентов УС ПУ $(u, v) \in T^M$;
- сформировать совокупность маскирующих $N_{ij}^{\text{маск}}$ маршрутов для передачи по ним маскирующих (ложных) сообщений между каждой парой абонентов УС ПУ $(u, v) \in T^M$;
- определить для каждого УС ИСС, принадлежащего маскирующим маршрутам, значения MTU;
- выбрать узлы-терминаторы G^T маскирующих сообщений в каждом маскирующем маршруте связи;
- при необходимости дополнительно согласовать между абонентами УС ПУ параметры TCP MSS (см., например, [32]);
- задать маркеры перегрузки каналов связи (ребер минимального остовного дерева) пакетами сообщений;
- реализовать маскирующий обмен между каждой парой абонентов по T^M до G^T.

Исходные данные.

Маршруты передачи трафика в полученной структуре сети маскирующего обмена T^M содержат транзитные узлы ССОП. Для каждого x-го узла связи, принадлежащего T^M, где $x = 1, 2,\ldots, X$, задают совокупность Y параметров безопасности и их значения b_{xy}, где $y = 1, 2,\ldots, Y$.

Совокупность возможных маршрутов связи между каждой парой i-м и j-м абонентами УС ПУ, принадлежащей T^M, где $i = 1, 2,\ldots$, $j = 1, 2,\ldots$, и $i \neq j$, задают в виде N_{ij} деревьев графа сети связи. Число N_{ij} деревьев графа сети связи между i-м и j-м абонентами сети вычисляют по формуле:

$$N_{ij} = \left| B_o \times B_o^{\mathrm{T}} \right|, \qquad (6)$$

где $\boldsymbol{B}_o = \boldsymbol{M} \times \boldsymbol{K}$ – преобразованная матрица смежности вершин графа сети связи, а $M = M_p - 1$; K – число строк и столбцов матрицы; M_p – число строк исходной матрицы смежности, равное общему количеству узлов сети связи; B_o^{T} – транспонированная матрица к B_o.

Показатели и критерии.

Комплексный показатель безопасности $k_{x\Sigma}$ для каждого x-го узла структуры сети маскирующего обмена вычисляют путем суммирования, или перемножения, или как среднее арифметическое значение его параметров безопасности b_{xy}.

Средний показатель безопасности маршрута $k_{ij}^{\text{ср}}$ для каждого из N_{ij} возможных маршрутов связи вычисляют как среднее арифметическое комплексных показателей безопасности $k_{x\Sigma}^{n}$ узлов сети, входящих в n-ый маршрут связи.

В качестве безопасного маршрута связи $N_{ij}^{\text{доп}}$ выбирают маршрут с наибольшим значением его среднего показателя безопасности: $k_{ijn}^{\text{ср}} \to \max$.

Допустимые маршруты $N_{ij}^{\text{доп}}$ со значениями средних показателей безопасности $k_{ij}^{\text{ср}} \geq k_{ij}^{\text{доп}}$, используемые для передачи по ним конструктивных сообщений.

Маскирующие маршруты $N_{ij}^{\text{маск}}$ со значениями средних показателей безопасности $k_{ij}^{\text{ср}} < k_{ij}^{\text{доп}}$, используемые для передачи по ним маскирующих (ложных) сообщений с целью введения нарушителей в заблуждение относительно структуры сети связи.

Количество L возможных допустимых маршрутов связи между каждой парой абонентов сети.

Количество G маскирующих маршрутов связи между каждой парой абонентов сети.

Теоретической основой методики является теория графов, теория алгоритмов и теория матроидов.

Для достижения цели методики осуществляют последовательность действий, представленную блок-схемой на рис. 7. В общем случае ИСС ВН строят для соединения абонентов посредством ССОП (например, Интернет), представляющей собой совокупность физических линий (каналов) связи, соединяющих собой X узлов сети в единую инфраструктуру.

Различные серверы цифровых систем связи могут быть доступны или выделенной совокупности абонентов, как например, сервер безопасности, или представлять собой общедоступные серверы ССОП (например, Интернет).

Целесообразно рассматривать случаи, когда количество узлов сети X больше двух.

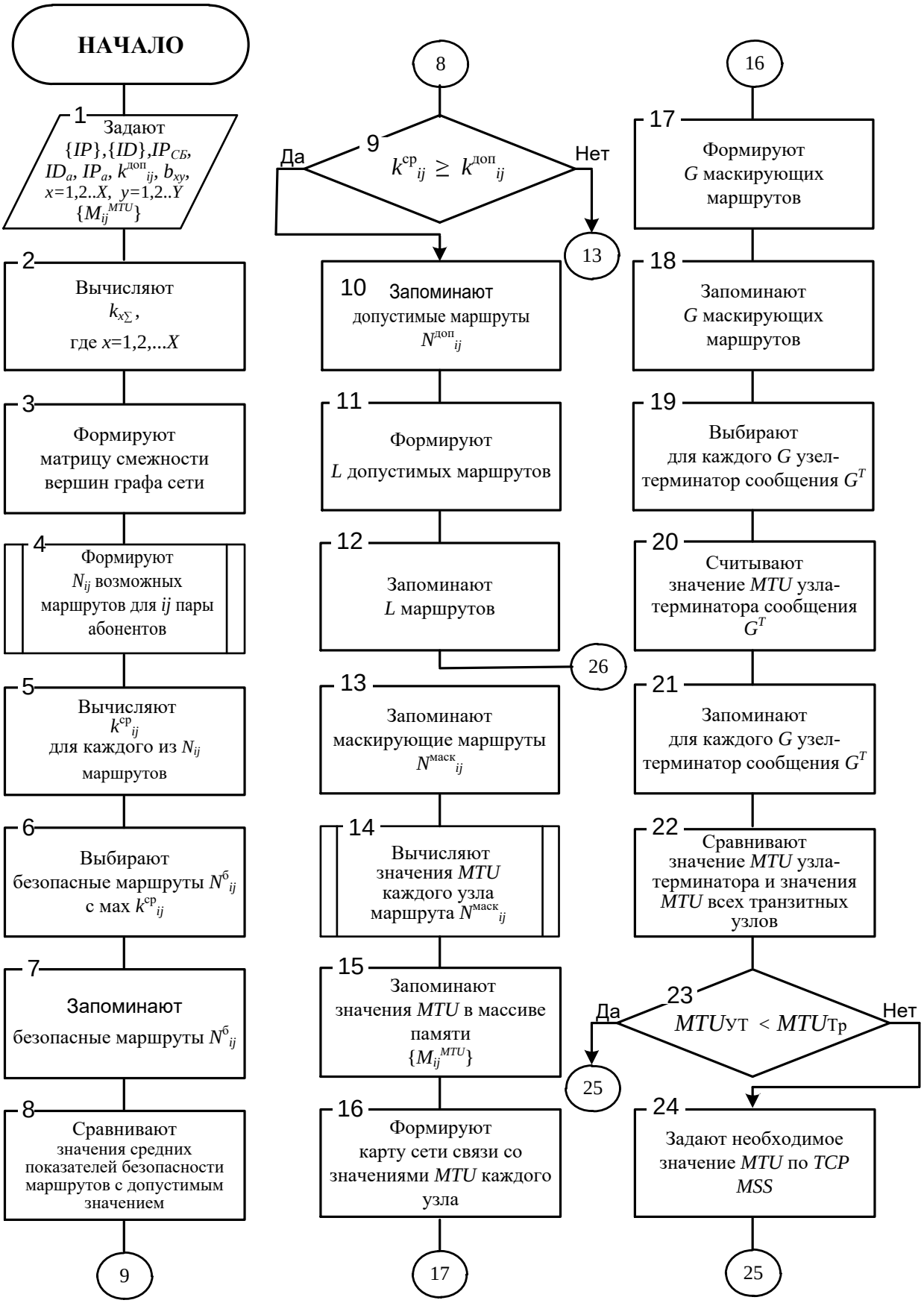

Рис. 7. Блок-схема алгоритма методики реализации маскирующего обмена (начало)

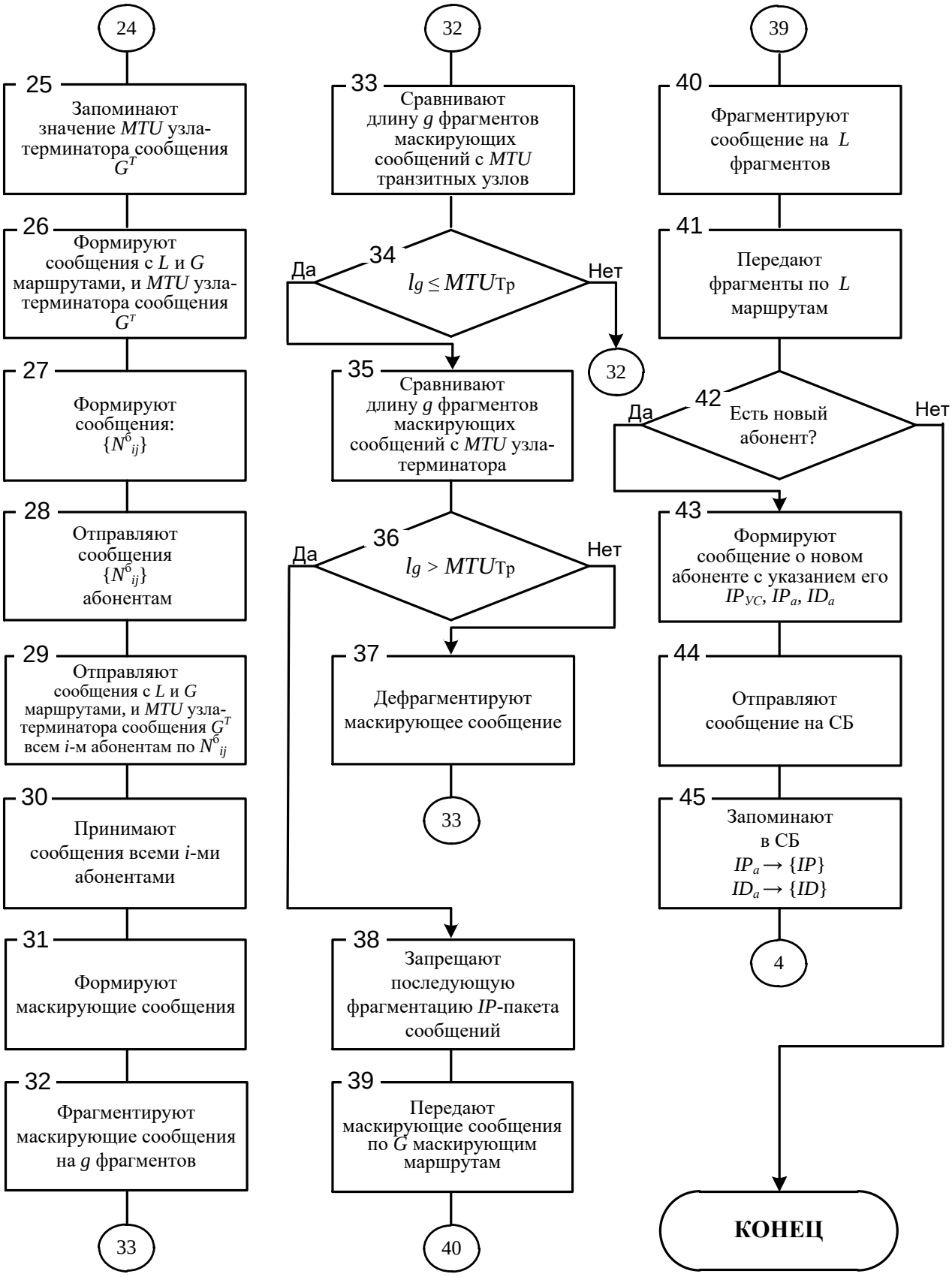

Рис. 7. Блок-схема алгоритма методики реализации маскирующего обмена (окончание)

Все элементы инфраструктуры определяются идентификаторами, в качестве которых в наиболее распространенном семействе протоколов TCP/IP используют сетевые адреса (IP- и MAC-адреса). При необходимости распределенной обработки информации и (или) ее передачи абоненты осуществляют подключение к ССОП. Множества адресов абонентов, подключенных к сети связи, и адресов узлов сети не пересекаются. При передаче пакетов сообщений по ССОП к абонентам сети, узлам сети и линиям (каналам) связи предъявляют требования информационной безопасности, характеризующие допустимые значения показателей безопасности элементов сети связи.

Рассмотрим для примера схему (граф) совокупности альтернативных маршрутов связи между парой абонентов УС ПУ $(u, v) \in T^M$, содержащую (рис. 8) транзитные узлы ССОП.

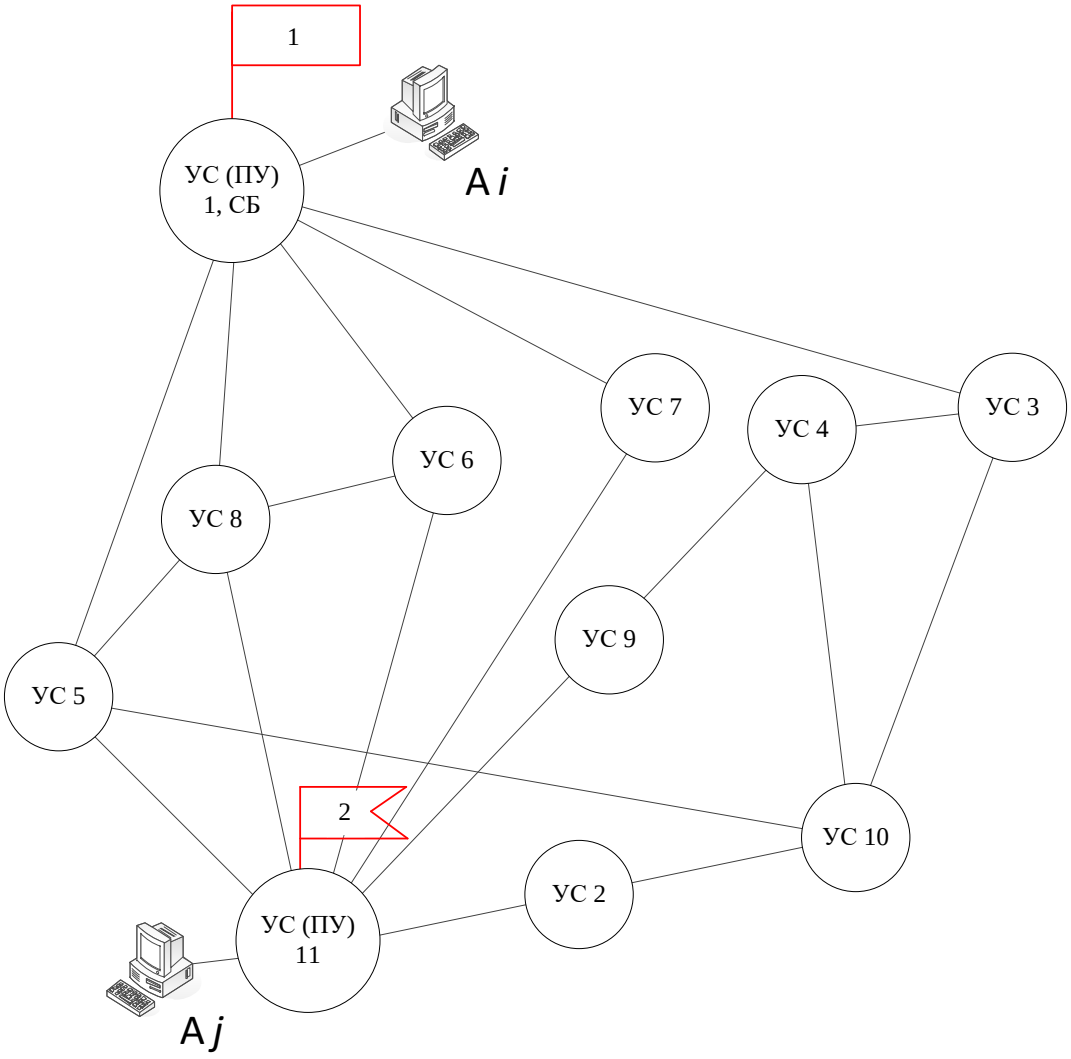

Рис. 8. Схема (граф) совокупности альтернативных маршрутов связи между парой абонентов ИСС ВН

Передача маскирующих сообщений, с помощью которых добиваются искажения структуры ИСС (алгоритмов функционирования) при ее реконструкции злоумышленником, может осуществляться между абонентами A_i и A_j. Возможен также вариант организации маскирующего обмена между абонентами A_i

или A_j и ложными абонентами A_f. Структура ССОП динамична и содержит большое количество узлов, поэтому задачи оценивания показателей безопасности, формирования маршрутов и обслуживания запросов абонентов о допустимых маршрутах связи целесообразно возлагать на выделенный сервер безопасности.

На начальном этапе в сервере безопасности задают исходные данные, включающие структурный $\{IP\}$ и идентификационный $\{ID\}$ массивы, адрес сервера безопасности $IP_{СБ}$, идентификаторы ID_a и адреса IP_a абонентов, подключенных к сети связи, массив памяти $\left\{M_{ij}^{MTU}\right\}$ для хранения вычисленных значений максимально возможной длины MTU пакета сообщений, который может быть передан без фрагментации узлами сети, принадлежащими маскирующему маршруту $N_{ij}^{маск}$. Для каждого x-го узла связи между парой абонентов $(u, v) \in T^M$, где $x = 1, 2, \ldots, X$, задают $Y \geq 2$ параметров безопасности и их значения b_{xy}, где $y = 1, 2, \ldots, Y$.

Параметры безопасности узлов ССОП определяют, например, в соответствии с ГОСТ Р ИСО/МЭК 15408-2002 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Значения b_{x1} параметра $y = 1$ безопасности узлов сети определяют, например, по характеристикам производителей оборудования узлов сети, информацию о которых можно получить из физических адресов узлов сети. Физические адреса узлов сети представляют в виде шестнадцатеричной записи, например 00:10:5a:3F:D4:E1, где первые три значения определяют производителя (00:01:e3 – Siemens, 00:10:5a – 3Com, 00:03:ba – Sun).

Также параметром безопасности узлов связи может являться местоположение и условия эксплуатации. Узлы связи могут находиться как в государственной организации или на объекте, на котором обрабатывают информацию, составляющую государственную тайну (то есть соблюдены требования по режиму секретности и противодействию техническим средствам разведки), или в частной организации, где соответствующие требования не выполняются.

В качестве остальных параметров безопасности узла ССОП можно рассматривать тип его оборудования, версию установленного на нем программного обеспечения, принадлежность узла государственной или частной организации и другие известные сведения.

Для каждого x-го узла связи между парой абонентов $(u, v) \in T^M$ по значениям b_{xy} его параметров безопасности вычисляют комплексный показатель безопасности $k_{x\sum}$.

Комплексный показатель безопасности $k_{x\sum}$ для каждого x-го узла сети вычисляют путем суммирования:

$$k_{x\sum} = \sum_{y=1}^{Y} b_{xy}, \quad (7)$$

или перемножения:

$$k_{x\sum} = \prod_{y=1}^{Y} b_{xy}, \quad (8)$$

или как среднее арифметическое значение:

$$k_{x\sum} = \left(\sum_{y=1}^{Y} b_{xy} \right) \Big/ Y \qquad (9)$$

его параметров безопасности b_{xy}.

Принципиально способ вычисления $k_{x\sum}$ не влияет на результат выбора безопасного маршрута.

Кроме этого возможен утилитарный подход к определению комплексных показателей безопасности $k_{x\sum}$ для каждого x-го узла сети, когда их задают бинарно-опасный узел, либо безопасный узел, в последнем случае полагая, что его безопасность доказана, но количественные значения показателей безопасности недоступны лицам, принимающим решение на выбор маршрута.

Пример расчета комплексных показателей безопасности узлов связи в соответствии с предложенной ранее структурой сети связи представлен в таблице 2.

Таблица 2 – Пример расчета комплексных показателей безопасности узлов связи

Узлы сети $X = 11$	Параметры безопасности узлов сети $Y = 3$			Комплексный показатель безопасности x-ого узла $k_{x\sum}$		
	$y = 1$	$y = 2$	$y = 3$	$\sum bxy$	$\prod bxy$	$(\sum bxy)/Y$
$x = 1$	0,8	0,9	0,7	2,4	0,50	0,8
$x = 2$	0,6	0,5	0,2	1,3	0,06	0,4
$x = 3$	0,2	0,3	0,2	0,7	0,01	0,2
$x = 4$	0,2	0,4	0,3	0,9	0,02	0,3
$x = 5$	0,7	0,8	0,7	2,2	0,39	0,7
$x = 6$	0,4	0,3	0,6	1,3	0,07	0,4
$x = 7$	0,3	0,3	0,5	1,1	0,05	0,4
$x = 8$	0,5	0,4	0,3	1,2	0,06	0,4
$x = 9$	0,5	0,3	0,5	1,3	0,08	0,4
$x = 10$	0,3	0,4	0,2	0,9	0,02	0,3
$x = 11$	0,8	0,8	0,7	2,3	0,45	0,8

Далее формируют матрицу смежности вершин графа сети [33], для чего запоминают в структурном массиве адреса узлов сети $IP_{УС}$ и адреса абонентов IP_a сети, а также информацию о наличии связи между узлами и абонентами сети.

После этого в идентификационном массиве запоминают идентификаторы ID_a, $ID_{СБ}$ и соответствующие им адреса IP_a, $IP_{СБ}$ абонентов сети и сервера безопасности.

Формируют совокупность возможных маршрутов связи между i-м и j-м абонентами ИСС ВН в виде N_{ij} деревьев графа сети связи. Каждое n-ое, где $n = 1, 2, \ldots, N_{ij}$, дерево графа состоит из z_n вершин, соответствующих количеству узлов сети информационного направления между i-м и j-м абонентами ИСС ВН. Порядок формирования деревьев графа известен и описан (см., например, [34]).

Построение маршрутов связи между абонентами на основе деревьев графа сети связи обеспечивает нахождение всех возможных маршрутов связи и их незамкнутость, т.е. исключает неприемлемые для передачи сообщений замкнутые маршруты.

Для обоснования и объективного выбора безопасного, допустимых и маскирующих маршрутов связи из совокупности N_{ij} возможных маршрутов связи между *i*-м и *j*-м абонентами сети вычисляют средние показатели безопасности $k_{ij}^{\text{ср}}$ как среднее арифметическое комплексных показателей безопасности k_{Σ}^{n} узлов сети, входящих в *n*-ый маршрут связи:

$$k_{ij}^{\text{ср}} = \left(\sum_{l=1}^{z} k_{\Sigma}^{n} \right) \Big/ z_n \, . \qquad (10)$$

Используя результаты, полученные при вычислении комплексных показателей безопасности узлов сети разными способами, вычисляются средние показатели безопасности $k_{ij}^{\text{ср}}$ маршрутов связи сформированных между *i*-м и *j*-м абонентами сети. В качестве безопасного маршрута выбирают и запоминают маршрут *n* с максимальным средним показателем безопасности.

Далее сравнивают значения средних показателей безопасности маршрутов $k_{ij}^{\text{ср}}$ с предварительно заданным допустимым значением $k_{ij}^{\text{доп}}$. Те маршруты, значения средних показателей безопасности которых удовлетворяют условию $k_{ij}^{\text{ср}} \geq k_{ij}^{\text{доп}}$, запоминают как допустимые маршруты $N_{ij}^{\text{доп}}$. Далее формируют совокупность возможных допустимых маршрутов связи *L* между каждой парой абонентов сети и запоминают сформированные *L* маршрутов.

Такие маршруты используют для передачи по ним конструктивного трафика. В том случае, если по результатам сравнения комплексных показателей безопасности маршрутов $k_{ij}^{\text{ср}}$ с предварительно заданным допустимым значением $k_{ij}^{\text{доп}}$ выявляют те маршруты, что удовлетворяют условию $k_{ij}^{\text{ср}} < k_{ij}^{\text{доп}}$, то такие маршруты запоминают как маскирующие $N_{ij}^{\text{маск}}$ маршруты.

Такие маршруты используют для передачи по ним маскирующих (ложных) сообщений. Таким образом, формируют множество маскирующих маршрутов между всеми абонентами сети.

Для иллюстрации примера расчетов в соответствии с предложенной ранее структурой сети связи сформируем совокупность возможных маршрутов связи между абонентами A_i, A_j и выявим среди них маскирующие (см. табл. 3).

В данном случае маскирующими маршрутами между абонентами A_i или A_j предлагается использовать маршруты №№ 7, 9, 12, 13.

После запоминания маскирующих маршрутов $N_{ij}^{\text{маск}}$ со значениями средних показателей безопасности $k_{ij}^{\text{ср}} < k_{ij}^{\text{доп}}$, строят карту сети со значениями *MTU* узлов сети, принадлежащих маскирующему маршруту, для чего вычисля-

ют значения MTU каждого узла сети, принадлежащего маскирующему маршруту $N_{ij}^{маск}$, и запоминают их в массиве памяти $\{M_{ij}^{MTU}\}$.

Таблица 3 – Расчет средних показателей безопасности маршрутов связи

Маршруты *Nij*=15	Номера узлов в *n*-м маршруте	Количество узлов *zn* в *n*-м маршруте	Средний показатель безопасности $k^{ср}_{ijn}$ *n*-ого маршрута		
n = 1	1-5-11	3	2,3	0,45	0,8
n = 2	1-8-11	3	2,0	0,34	0,7
n = 3	1-6-11	3	2,0	0,34	0,7
n = 4	1-7-11	3	1,9	0,33	0,6
n = 5	1-5-8-11	4	2,0	0,35	0,7
n = 6	1-8-6-11	4	1,8	0,27	0,6
n = 7	1-3-4-9-11	5	1,5	0,21	0,5
n =8	1-5-8-6-11	5	1,9	0,30	0,6
n = 9	1-3-10-2-11	5	1,5	0,21	0,5
n = 10	1-5-10-2-11	5	1,8	0,29	0,6
n = 11	1-3-10-5-11	5	1,7	0,28	0,6
n = 12	1-3-4-10-2-11	6	1,4	0,18	0,5
n = 13	1-3-10-4-9-11	6	1,4	0,18	0,5
n = 14	1-5-10-4-9-11	6	1,7	0,24	0,6
n = 15	1-5-10-4-9-11	6	1,7	0,2	0,6

Каждому каналу сети связи (определяется по передающему интерфейсу узла сети – маршрутизатора) соответствует максимальный размер передаваемого блока данных (MTU, Maximum Transmission Unit). Каждый сегмент передаваемых данных должен помещаться в MTU, чтобы он мог передаваться в одном пакете, не разделенном на фрагменты [35]. Для вычисления значения MTU каждого узла сети, принадлежащего маскирующему маршруту, применяют процедуру Path MTU Discovery, как это описано, например, в технических спецификациях (RFC, Request for Comments) сети Интернет [31].

Для передачи маскирующих (ложных) сообщений с целью введения нарушителей в заблуждение относительно структуры сети связи формируют совокупность возможных маскирующих маршрутов связи *G* между каждой парой абонентов сети и запоминают сформированные *G* маршруты.

После запоминания сформированных *G* маскирующих маршрутов связи выбирают для каждого маскирующего маршрута связи *G* узел-терминатор маскирующего сообщения G^T и запоминают его. Выбор узла-терминатора маскирующего сообщения G^T необходим для того, чтобы улучшить показатель своевременности доставки пакетов сообщений принимающему абоненту. Этого достигают тем, что пакеты маскирующих сообщений не будут доставляться принимающему абоненту (если он не является ложным), а будут уничтожаться на узле-терминаторе. В результате принимающий абонент не будет перегружен маскирующими сообщениями, и показатель своевременности доставки ему конструктивных (не маскирующих) сообщений будет улучшен.

В том случае, если принимающий абонент является ложным, то в каче-

стве узла-терминатора маскирующего сообщения G^T выбирают принимающего абонента.

Затем считывают из массива памяти $\left\{M_{ij}^{\text{MTU}}\right\}$ значение MTU узла-терминатора маскирующего сообщения G^T и запоминают его. В качестве узла-терминатора маскирующего сообщения G^T выбирают узел сети, принадлежащий маскирующему маршруту связи, который прекращает дальнейшую передачу пакетов маскирующих сообщений, если длина g-го фрагмента сообщения больше принятого на узле-терминаторе значения MTU. При сравнении длины g-го фрагмента сообщения с принятым значением MTU узла-терминатора маскирующего сообщения G^T учитывают длину служебной части пакета сообщения, добавляемую при передаче адресату к каждому пакету сообщений.

С одной стороны значение MTU маскирующего пакета сообщений должно быть меньшим или равным минимальному значению MTU на всем маршруте следования пакета до узла-терминатора. С другой стороны значение MTU маскирующего пакета сообщений должно быть большим чем значение MTU узла-терминатора, чтобы маскирующий трафик не доходил до получателя. При использовании только Path MTU Discovery возможно нахождение наименьшего значения MTU на промежуточном интервале. В этом случае маскирующий трафик будет терминироваться на транзитном узле, не доходя до узла-терминатора.

В связи с этим, если минимальное значение MTU находится не на узле, где мы планируем назначить узел-терминатор маскирующего трафика, предлагается дополнительно согласовывать между абонентами TCP MSS и задавать необходимое его значение. Суть процедуры TCP MSS заключается в определении максимального размера данных, который машина готова получить через один TCP сегмент. Сам TCP сегмент инкапсулируется в IP-пакет. Значение MSS передается в заголовке TCP SYN при установлении соединения между двумя узлами (через механизм трехэтапного установления соединения).

Далее формируют сообщения, включающие запомненные безопасные $N_{ij}^{\text{б}}$, допустимые и маскирующие маршруты между i-м и всеми j-ми абонентами, идентификаторы ID_{aj} и адреса IP_{aj} всех j-х абонентов, а также значение MTU узла-терминатора маскирующего сообщения G^T между i-м и всеми j-ми абонентами. Отправляют сформированные сообщения по безопасным маршрутам всем i-м абонентам сети и принимают их абонентами сети. Для передачи сообщений между абонентами по безопасному маршруту по идентификатору абонента-получателя сообщения ID_a выбирают его адрес IP_a и безопасный маршрут $N_{ij}^{\text{б}}$.

Таким образом, каждого абонента сети уведомляют о безопасных, допустимых и маскирующих маршрутах ко всем остальным абонентам, а также о значениях MTU, которые необходимо устанавливать для маскирующих сообщений, чтобы они уничтожались на выбранном узле-терминаторе каждого маскирующего маршрута.

Исходящие сообщения фрагментируют на L фрагментов и передают фрагменты сообщения по L возможным допустимым маршрутам связи. При подключении нового абонента к сети связи ему доводятся сообщения о безопас-

ном, допустимых L и маскирующих G маршрутах ко всем абонентам сети, а остальных абонентов уведомляют о безопасном, допустимых L и маскирующих G маршрутах к новому абоненту.

Для формирования маскирующих сообщений генерируют ложные исходные пакеты данных, в информационную часть которых записывают случайную или произвольную цифровую последовательность (случайную последовательность сигналов логический «0» и логическая «1»).

После формирования маскирующих сообщений, содержащих маскирующую информацию, фрагментируют маскирующие сообщения на g фрагментов. Фрагментация маскирующих сообщений необходима для уменьшения среднего времени нахождения в очереди конструктивных (немаскирующих) пакетов, имеющих больший приоритет при отправке в сеть. Однако фрагментированные маскирующие сообщения могут иметь длину меньшую, чем MTU узла-терминатора или большую чем MTU транзитных узлов. Следовательно, маскирующий трафик будет доходить до конечного абонента или будет терминироваться на другом транзитном узле, что не будет соответствовать замыслу введения в заблуждение противника.

Для устранения этого противоречия необходимо сравнивать длину каждого g-го фрагмента с принятым значением MTU узла-терминатора маскирующего сообщения G^T, а также MTU транзитных узлов. Сравнение необходимо для того, чтобы определить, будет ли уничтожен пакет маскирующего сообщения на узле-терминаторе. При сравнении длины g-го фрагмента маскирующего сообщения с принятыми значениями MTU узла-терминатора и транзитных узлов учитывают длину служебной части пакета сообщения, добавляемую при передаче адресату к каждому пакету сообщений. И в случае, если длина g-го фрагмента больше принятого значения MTU узла-терминатора маскирующего сообщения G^T и меньше или равна значений MTU транзитных узлов, то запрещают последующую фрагментацию IP-пакета сообщений при его передаче по сети связи. Для запрещения фрагментации IP-пакета сообщений при его передаче по сети связи устанавливают в единицу значение флага DF (Do not Fragment) «не фрагментировать» в заголовке IP-пакета сообщений. Установка этого флага в единицу означает запрет последующей фрагментации [36], что приводит к запрету ретрансляции пакета сообщений дальше узла-терминатора. Затем передают сформированные маскирующие сообщения по выбранному маскирующему маршруту связи.

В противном случае, то есть, если длина g-го фрагмента меньше или равна принятому значению MTU узла-терминатора маскирующего сообщения G^T, то дефрагментируют маскирующее сообщение. Для чего объединяют между собой два или более фрагмента маскирующих сообщений, но с таким условием, что длина g-го фрагмента маскирующего сообщения будет меньше или равна значений MTU транзитных узлов.

Таким образом, за счет динамического изменения длины пакетов маскирующих сообщений, достигают уменьшения среднего времени ожидания в очереди пакетов сообщений у передающего абонента.

Маскирующий обмен реализуется между каждой парой абонентов УС ПУ или от точек истока по T^M до G^T. При этом маскирование между абонентами может осуществляться в зависимости от замысла обмана:

как по одному маршруту, так и по нескольким (тогда заданную интенсивность МО необходимо разделить на количество задействованных в обмене маршрутов);

в специально выделенный промежуток времени (в этом случае необходимо иметь уверенность в том, что именно в этот момент времени был обеспечен контакт технического средства разведки с каналом связи), или постоянно, но не превышая рассчитанной максимальной нагрузки.

Итоговая схема связи между абонентами A_i или A_j, включающая допустимые и маскирующие маршруты представлена на рис. 9.

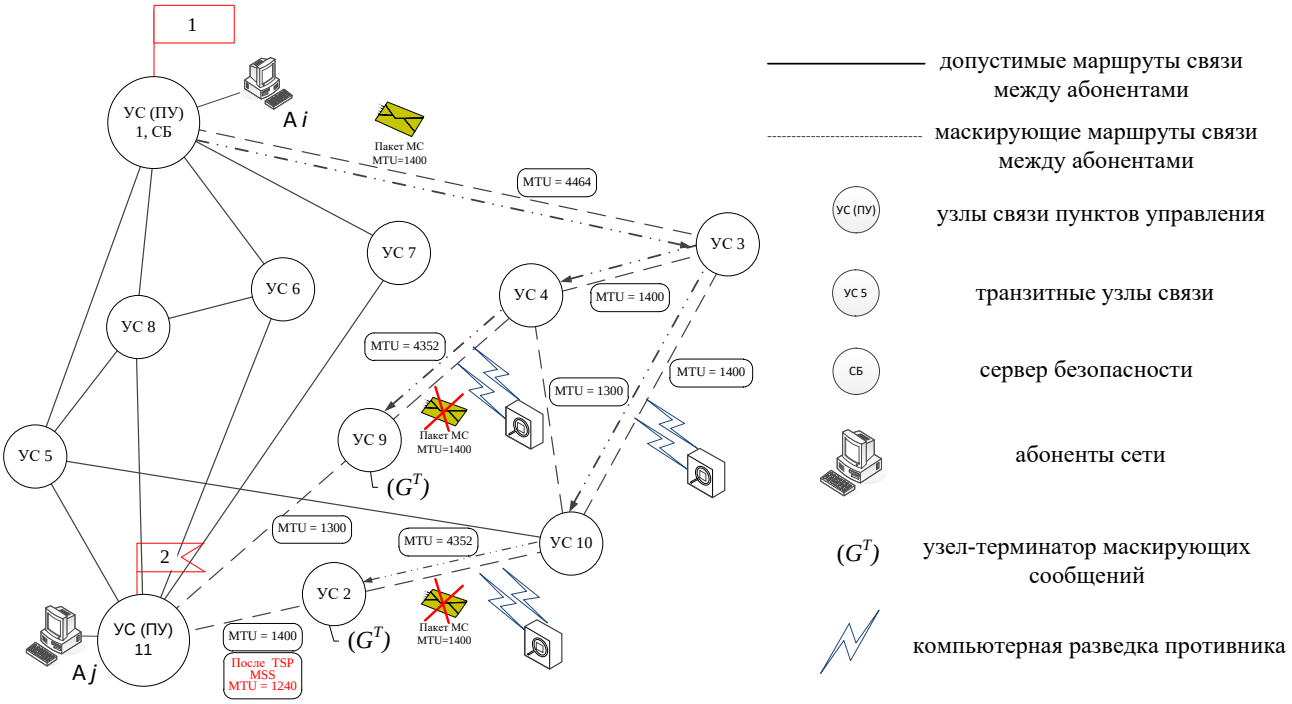

Рис. 9. Итоговая схема связи между абонентами A_i или A_j

Результаты моделирования

Результаты использования методики могут быть проверены при помощи эксперимента на имитационной модели. Это необходимо для того, чтобы учесть случайные помехи среды ССОП, и получить численную оценку выигрыша от ее применения.

В качестве программного обеспечения которой используется объектно-ориентированная среда моделирования UNetLab, где все объекты сети задаются и настраиваются по параметрам.

Экспериментальный макет ИСС ВН представлен 9-ю абонентами УС ПУ и объединяющей их сетью (рис. 10). Абоненты УС соответствующих ПУ обмениваются двумя видами трафика в обоих направлениях. Один вид трафика представляет собой полезную нагрузку, другой – маскирующий обмен.

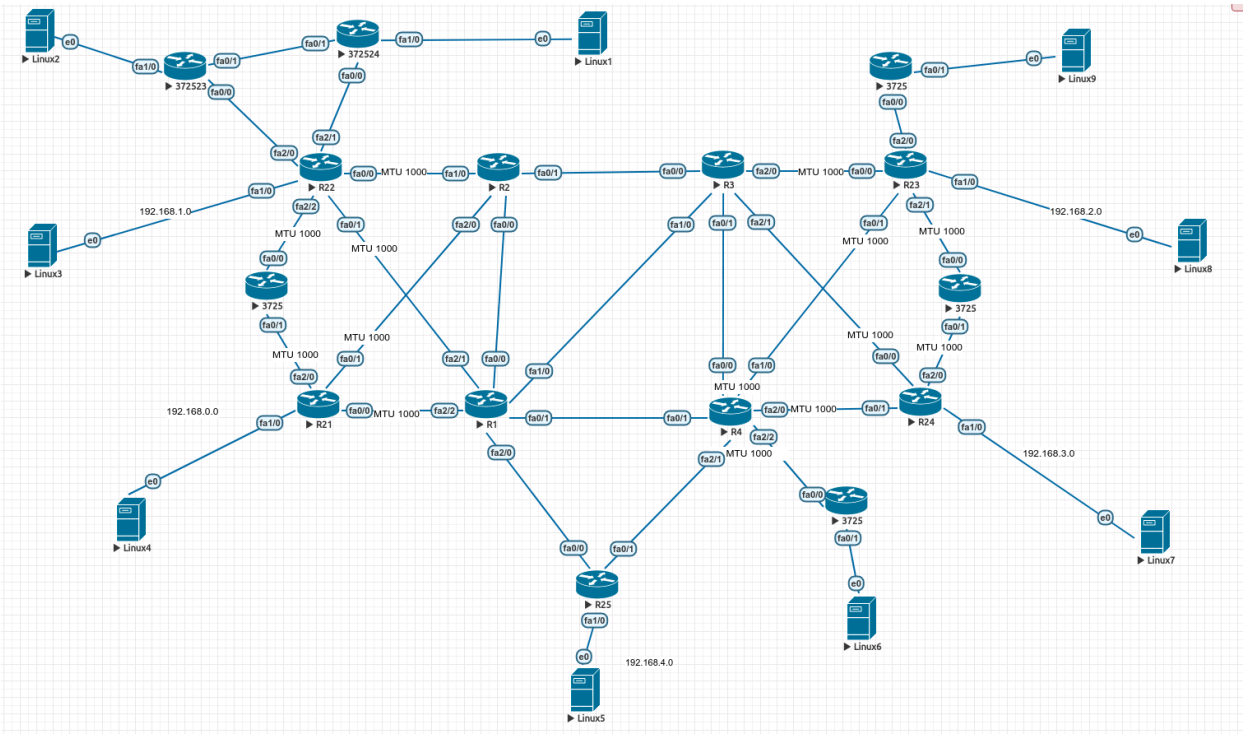

Рис. 10. Схема экспериментального макета ИСС ВН

Маскирующий трафик, в свою очередь, может либо свободно поступать от одного узла к другому, либо прерываться на некотором участке сети (узле-терминаторе). График изменения интенсивности конструктивного и маскирующего трафика при смене режимов функционирования в реальном времени представлен на графике (рис. 11).

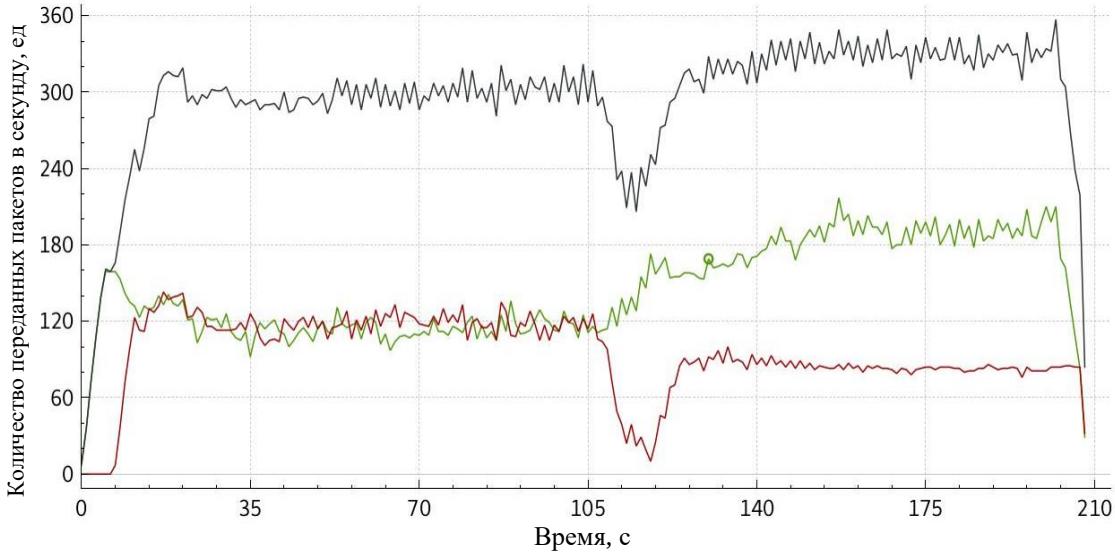

Рис. 11. График изменения интенсивности конструктивного и маскирующего трафика при смене режимов функционирования в реальном времени

Как видно из графика, ограничение маскирующего трафика (красная кривая) узлом-терминатором, позволяет снизить данный тип трафика, и тем самым освободить ресурсы для увеличения скорости передачи полезного трафика (зе-

леная кривая). Что повышает производительность системы при сохранении функции маскирования.

В результате моделирования получены зависимости, представленные на графике, которые построены на основании усредненной тенденции изменения интенсивности трафика при смене режимов (с ограничением маскирующего трафика и без ограничения) и изменении количества узлов (рис. 12).

Чтобы оценить эффективность информационного обмена с точки зрения его своевременности вводится показатель $T_{\text{Д}}$ – время передачи 1 Мбит конструктивного трафика.

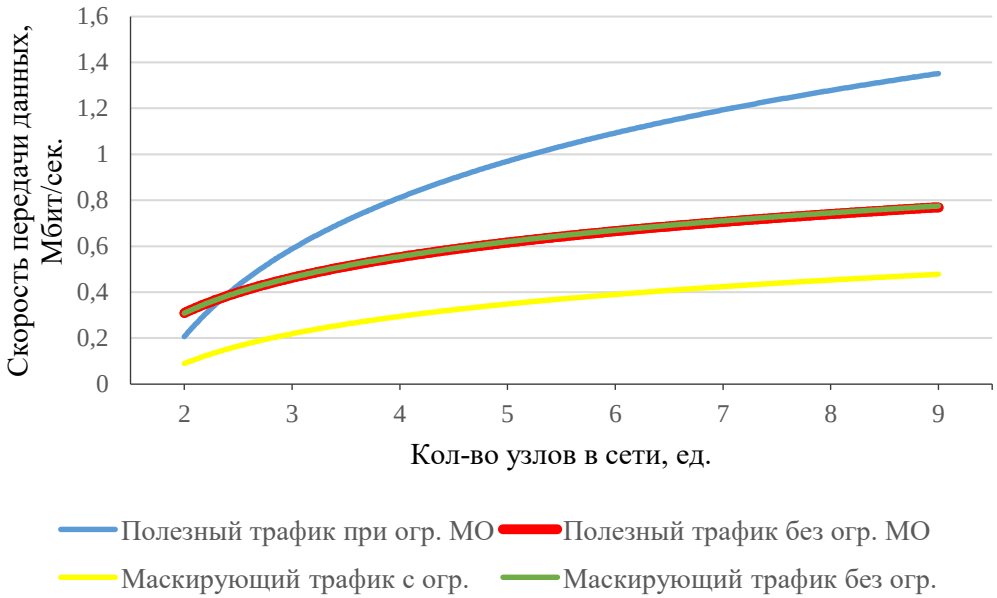

Рис. 12. Результаты эксперимента по оценки влияния маскирующего трафика на производительность ИСС ВН

Тогда коэффициент эффективности информационного обмена с учетом влияния маскирующего трафика в *i*-ом испытании:

$$K_i^{\text{Эф}} = \frac{\overline{T}_{i\text{ИО}}^{\text{ОТ}} - \overline{T}_{i\text{ИО}}^{\text{КТ}}}{\overline{T}_{i\text{ИО}}^{\text{ОТ}}} \cdot 100\%, \qquad (11)$$

где $\overline{T}_{i\text{ИО}}^{\text{ОТ}}$ – среднее время информационного обмена общим трафиком (конструктивным и маскирующим); $\overline{T}_{i\text{ИО}}^{\text{КТ}}$ – среднее время информационного обмена конструктивным трафиком при ограничении МО узлами-терминаторами. В результате моделирования получены значения коэффициента эффективности информационного обмена, которые представлены в таблице 4.

Таблица 4 – Результаты имитационного моделирования

№ эксперимента	Кол-во хостов в целевой подсети; № испытания	Полезный трафик при ограничении МО			Полезный трафик без ограничения МО			Коэффициент эффективности информационного обмена, %
		Скорость передачи, Мбит/сек	Время передачи 1 Мбит, сек	Среднее время передачи 1 Мбит, сек	Скорость передачи, Мбит/сек	Время передачи 1 Мбит, сек	Среднее время передачи 1 Мбит, сек	
1	2;1	0,268726408	3,721256897	3,719312767	0,263847795	3,79006389	3,730875601	0,31%
	2;2	0,271115556	3,688464121		0,262976376	3,802622936		
	2;3	0,259342598	3,855903383		0,269217037	3,714475178		
	2;4	0,278445944	3,591361345		0,271764918	3,679650809		
	2;5	0,267409846	3,739578089		0,272660457	3,667565191		
2	3;1	0,542008975	1,844987897	1,853226101	0,538964058	1,855411294	1,872449022	1,03%
	3;2	0,54327382	1,840692416		0,537521532	1,86039059		
	3;3	0,542908687	1,841930371		0,522209019	1,914942031		
	3;4	0,53939209	1,853938939		0,529934144	1,887026927		
	3;5	0,530621959	1,884580882		0,542159908	1,84447427		
3	4;1	0,500511901	1,99795449	1,78067592	0,465905103	2,146359833	1,873559833	4,96%
	4;2	0,61545848	1,624804974		0,653676981	1,529807579		
	4;3	0,578869741	1,727504357		0,644746631	1,550996859		
	4;4	0,558444447	1,790688412		0,485066636	2,061572422		
	4;5	0,567399269	1,762427369		0,480986028	2,07906247		
4	5;1	0,639256094	1,56431829	1,527435682	0,562053814	1,779189066	1,687943075	9,51%
	5;2	0,631912979	1,582496377		0,596820821	1,675544761		
	5;3	0,654284559	1,528386979		0,603671584	1,656529853		
	5;4	0,614822265	1,626486315		0,581869883	1,718597284		
	5;5	0,748788583	1,335490448		0,621174184	1,609854412		
5	6;1	0,803038563	1,245270209	1,236373346	0,641799976	1,558117851	1,475043754	16,18%
	6;2	0,746497536	1,339589151		0,689375237	1,450588803		
	6;3	0,805754905	1,241072185		0,66513174	1,503461555		
	6;4	0,797786055	1,253468888		0,642096314	1,557398756		
	6;5	0,907057209	1,102466295		0,765900982	1,305651806		
6	7;1	0,880170313	1,13614375	1,069706802	0,705473085	1,417488521	1,457872915	26,63%
	7;2	0,943184796	1,060237616		0,668968277	1,494839193		
	7;3	1,053045443	0,949626634		0,659937724	1,515294495		
	7;4	0,913352562	1,09486746		0,685740721	1,458277114		
	7;5	0,902805293	1,107658548		0,712522095	1,40346525		
7	8;1	1,048758099	0,953508727	0,897174452	0,753873596	1,326482325	1,368472827	34,44%
	8;2	0,958826232	1,042941846		0,715815705	1,397007628		
	8;3	1,210275783	0,82625796		0,749332119	1,334521735		
	8;4	1,216311688	0,822157684		0,719773694	1,389325574		
	8;5	1,189052095	0,841006045		0,716832068	1,395026875		
8	9;1	1,05191309	0,950648879	0,813606883	0,739500596	1,352263954	1,300966613	37,46%
	9;2	1,186085833	0,843109303		0,803584791	1,244423751		
	9;3	1,154212785	0,866391374		0,744951633	1,342369028		
	9;4	1,466215195	0,682028125		0,756893562	1,32118973		
	9;5	1,377682336	0,725856733		0,803479644	1,244586601		

Проведенный анализ результатов показывает, что время передачи 1 Мбит конструктивного трафика при вводе узлов-терминаторов уменьшается в среднем на 25 % от реализации маскирующего обмена без них. Что обеспечивает

своевременность доставки сообщений абонентам сети при реализации маскирующего обмена.

Для оценки достоверности результатов имитационного моделирования использован *t*-критерий Стьюдента.

Формула расчета *t*-критерия Стьюдента имеет вид:

$$t = \frac{\left|M_1 - M_2\right|}{\sqrt{\frac{s_1^{\,2}}{N_1} + \frac{s_2^{\,2}}{N_2}}}, \tag{12}$$

Однако, при анализе выборок математическое ожидание не известно, поэтому полагаем, что $M_1 = \bar{X}_1, M_2 = \bar{X}_2,$ тогда вместо дисперсии используем выборочную дисперсию:

$$s_1^{\,2} = \frac{\sum_{i=1}^{N_1}(X_i - \bar{X}_1)^2}{N_1},\ s_2^{\,2} = \frac{\sum_{i=1}^{N_2}(X_i - \bar{X}_2)^2}{N_2}, \tag{13}$$

Следовательно формула расчета *t*-критерия будет иметь следующий вид:

$$t = \frac{\left|\bar{X}_1 - \bar{X}_2\right|}{\sqrt{\frac{s_1^{\,2}}{N_1} + \frac{s_2^{\,2}}{N_2}}}, \tag{14}$$

где $\bar{X}_i$ – среднее выборочное; $s_i^{\,2}$ – выборочная дисперсия; N_i – объем выборки.

Среднее *P*-значение *t*-критерия Стьюдента при реализации конструктивного трафика по результатам серии экспериментов составило 0,021982. Следовательно, получены статистически значимые различия во времени передачи конструктивного трафика с ограничением маскирующего обмена и без такового.

В результате можно констатировать, что уменьшение времени передачи конструктивного трафика при осуществлении маскирующего обмена вызвано последовательностью действий в соответствии с предлагаемой методикой, что подтверждает сформулированную гипотезу.

Это позволяет сделать вывод, что результаты, полученные в ходе имитационного моделирования, не являются случайными, а являются результатами действий в соответствии с данной методикой.

Научная новизна методики заключается в применении модифицированных алгоритмов минимальных остовных деревьев и дифференциации маршрутов между УС ПУ по критерию безопасности транзитных узлов связи для реализации маскирующего обмена в ИСС ВН.

Практическая значимость предложенной методики заключается в снижении нагрузки абонентов сети обработкой маскирующих сообщений и обеспечении своевременности доставки сообщений при осуществлении маскирующего обмена при защите алгоритмов функционирования ИСС ВН от компьютерной разведки.

Заключение

Представленный научно-методический аппарат позволяет при защите от компьютерной разведки искажать алгоритмы функционирования ИСС ВН по заданным требованиям (в соответствии с замыслом обмана), снижать нагрузку на абонентов сети и обеспечивать своевременность доставки сообщений при осуществлении маскирующего обмена. Исследованиям, посвященным маскированию структуры сетей связи посвящено множество работ [20, 23-25].

Наиболее близким аналогом по своей технической сущности к представленной методике является [24], где обеспечивают повышение скрытности связи и затруднение идентификации абонентов сети несанкционированными абонентами за счет непрерывного изменения идентификаторов абонентов сети в передаваемых пакетах сообщений, передачу пакетов сообщений по всем допустимым маршрутам связи и передачу маскирующих сообщений по маскирующим маршрутам связи. Однако, недостатками указанного аналога являются относительно высокая перегрузка абонентов сети обработкой маскирующих сообщений, обусловленная возможностью образования очередей пакетов сообщений у передающего абонента, занятого обработкой и передачей в сеть связи маскирующих сообщений, и ухудшение показателя своевременности доставки пакетов сообщений принимающему абоненту, что может привести к потере фрагментов пакетов сообщений, вызванной истечением предельно допустимого времени их пребывания на маршруте связи. Повторная передача потерянных пакетов сообщений приводит к дополнительной нагрузке на сеть связи и абонентов, а повторная передача потерянных маскирующих пакетов сообщений может привести к компрометации результатов маскирования структуры сети связи. Указанные недостатки могут быть решены применением указанного научно-методического аппарата.

Литература

1. Давыдов А.Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М.: ОАО «Воентелеком», 2015. – 520 с.

2. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Безопасность ведомственных интегрированных инфокоммуникационных систем: учебное пособие. – СПб.: ФГУП «НИИ «Масштаб», 2011. – 192 с.

3. Голуб Б. В., Кузнецов Е. М., Максимов Р. В. Методика оценки живучести распределенных информационных систем // Вестник Самарского государственного университета. 2014. № 7 (118). С. 221-232.

4. Искольный Б. Б., Максимов Р. В., Шарифуллин С. Р. Оценка живучести распределенных информационно-телекоммуникационных сетей // Вопросы кибербезопасности. 2017. № 5 (24). С. 72-82. doi: 10.21681/2311-3456-2017-5-72-82.

5. Максимов Р. В., Павловский А. В., Самохин В. Ф., Чернолес В. П. Информационная безопасность России в сфере науки и техники // Информация и космос. 2006. № 4. С. 94-102.

6. Максимов Р. В., Соколовский С. П., Шарифуллин С. Р., Чернолес В. П. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3 (233). С. 28-35.

7. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure In-formation Technologies» (BIT 2017). Bauman Moscow Technical University, 2017, pp. 59-65.

8. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации [Электронный ресурс]. 2016. – URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения 01.09.2018).

9. Maximov R. V., Sokolovsky S. P., Gavrilov A. L. Hiding computer network proactive security tools unmasking features // Selected Papers of the VIII All-Russian Conference with International Participation “Secure In-formation Technologies” (BIT 2017). Bauman Moscow Technical University, 2017, pp. 88-92.

10. Выговский Л. С., Максимов Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости СПбГПУ. 2008. № 3 (60). С. 166-173.

11. Выговский Л. С., Максимов Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости СПбГПУ. 2009. № 1 (73). С. 181-187.

12. Максимов Р. В., Савинов Е. А. Оценка живучести распределенных интегрированных информационных систем // Информационные технологии и нанотехнологии (ИТНТ-2016). Материалы Международной конференции и молодежной школы. – Самара: Самарский государственный аэрокосмический университет имени академика С.П. Королева (национальный исследовательский университет). Институт систем обработки изображений РАН, 2016. С. 431-438.

13. Максимов Р. В., Апарин Н. Н., Астахов А. И., Жираковский А. А., Игнатенко А. В., Костырев А. Л., Нехаев М. А. Способ сравнительной оценки структур сетей связи // Патент на изобретение RU 2460123, опубл. 27.08.2012, Бюл. № 24, 19 с.

14. Максимов Р. В., Игнатенко А. В., Ковалевский С. Г., Озеров О. В., Тевс О. П., Шляхтенко Д. Б. Способ сравнительной оценки структур сетей связи // Патент на изобретение RU 2450338, опубл. 10.05.2012, Бюл. № 13, 16 с.

15. Максимов Р. В., Берест П. А., Богачев К. Г., Выговский Л. С., Игнатенко А. В., Кожевников Д. А., Краснов В. А., Кузнецов В. Е. Способ сравнительной оценки структур информационно-вычислительной сети // Патент на изобретение RU 2408928, опубл. 10.01.2011, Бюл. № 1, 16 с.

16. Максимов Р. В., Кожевников Д. А., Павловский А. В. Способ защиты вычислительной сети (варианты) // Патент на изобретение RU 2325694, опубл. 27.05.2008, Бюл. № 15, 106 с.

17. Максимов Р. В., Кожевников Д. А., Павловский А. В., Юрьев Д. Ю. Способ выбора безопасного маршрута в сети связи (варианты) // Патент на изобретение RU 2331158, опубл. 10.08.2008, Бюл. № 22, 34 с.

18. Максимов Р. В., Андриенко А. А., Кожевников Д. А., Колбасова Г. С., Павловский А. В., Стародубцев Ю. И. Способ (варианты) и устройство (варианты) защиты канала связи вычислительной сети // Патент на изобретение RU 2306599, опубл. 20.09.2007, Бюл. № 26, 56 с.

19. Максимов Р. В., Ветошкин И. С., Дрозд Ю. А., Ефимов А. А., Игнатенко А. В., Кожевников Д. А., Краснов В. А., Кузнецов В. Е. Способ защиты вычислительной сети с выделенным сервером // Патент на изобретение RU 2449361, опубл. 10.02.2011, Бюл. № 4, 16 с.

20. Максимов Р. В., Голуб Б. В., Горячая А. В., Кожевников Д. А., Лыков Н. Ю., Тихонов С. С. Способ маскирования структуры сети связи // Патент на изобретение RU 2622842, опубл. 20.06.2017, Бюл. № 17, 21 с.

21. Максимов Р. В., Искольный Б. Б., Лазарев А. А., Лыков Н. Ю., Хорев Г. А., Шарифуллин С. Р. Способ сравнительной оценки структур сетей связи // Патент на изобретение RU 2626099, опубл. 21.07.2017, Бюл. № 21, 19 с.

22. Максимов Р. В., Орехов Д. Н., Проскуряков И. С., Соколовский С. П. Способ защиты вычислительных сетей // Патент на изобретение RU 2649789, опубл. 04.04.2018, Бюл. № 10, 25 с.

23. Дыбко Л. К., Иванов И. И., Лыков Н. Ю., Максимов Р. В., Проскуряков И. С., Хорев Г. А., Шарифуллин С. Р. Способ маскирования структуры сети связи // Патент на изобретение RU 2656839, опубл. 06.06.2018, Бюл. № 16, 27 с.

24. Голуб Б. В., Краснов В. А., Лыков Н. Ю., Максимов Р. В. Способ маскирования структуры сети связи // Патент на изобретение RU 2645292, опубл. 19.02.2018, Бюл. № 5, 29 с.

25. Белов А. А., Иванов И. И., Лазарев А. А., Максимов Р. В., Мирошниченко Е. Л., Шарифуллин С. Р. Способ маскирования структуры сети связи // Патант на изобретение RU 2668979, опубл. 05.10.2018, Бюл. № 28, 29 с.

26. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.

27. Максимов Р. В., Выговский Л. С., Заргаров И. А., Кожевников Д. А., Павловский А. В., Стародубцев Ю. И., Худайназаров Ю. К., Юров И. А. Способ (варианты) защиты вычислительных сетей // Патент на изобретение RU 2307392, опубл. 27.09.2007, Бюл. № 27, 22 с.

28. Максимов Р. В., Андриенко А. А., Куликов О. Е., Костырев А. Л., Павловский А. В., Лебедев А. Ю. Способ контроля информационных потоков в цифровых сетях связи // Патент на изобретение RU 2267154, опубл. 27.12.2005, Бюл. № 36, 16 с.

29. Максимов Р. В., Андриенко А. А., Куликов О. Е., Костырев А. Л. Способ обнаружения удаленных атак на автоматизированные системы

управления // Патент на изобретение RU 2264649, опубл. 20.11.2005, Бюл. № 32, 15 с.

30. Maximov R. V., Ivanov I. I., Sharifullin S. R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University, 2017, pp. 83-87.

31. RFC 1191. Path MTU Discovery. Draft Standard. 1990. URL: http://tools.ietf.org/html/rfc1191 (дата обращения 04.09.2018).

32. RFC 879. The TSP Maximum Segment Size and Related Topics. 1983. URL: http://tools.ietf.org/html/rfc879#section-3 (дата обращения 06.09.2018).

33. Басакер Р., Саати Т. Конечные графы и сети. – М.: Наука, 1973. – 38 с.

34. Кристофидес Н. Теория графов: Алгоритмический подход. Пер. с англ. – М.: Мир, 1978. – 432 с.

35. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2017. – 90 с.

36. RFC 791. DARPA internet program protocol specification. Enternet Standard. 1981. – URL: http://tools.ietf.org/html/rfc791 (дата обращения 06.09.2018).

References

1. Davydov A. E., Maximov R. V., Savickij O. K. *Zashchita i bezopasnost' vedomstvennyh integrirovannyh infokommunikacionnyh sistem* [The Protection and Security of Departmental Integrated Information and Communication Systems]. Moscow, Plc «Voentelekom», 2015. 520 p. (in Russian).

2. Davydov A. E., Maximov R. V., Savickij O. K. *Bezopasnost' vedomstvennyh integrirovannyh infokommunikacionnyh system* [Security of Departmental Integrated Information Communication Systems]. Saint-Petersburg, Federal State Unitary Enterprise «Research Institute «Masshtab», 2011. 192 p. (in Russian).

3. Golub B. V., Kuznecov E. M., Maximov R. V. Metodika ocenki zhivuchesti raspredelennyh informacionnyh system [Methodology of Assessing the Survivability of Distributed Information Systems]. *Vestnik of Samara state University*, 2014, vol. 118, no. 7, pp. 221-232 (in Russian).

4. Iskol'nyj B. B., Maximov R. V., Sharifullin S. R. Ocenka zhivuchesti raspredelennyh informacionno-telekommunikacionnyh setej [Evaluation of Survivability of Distributed Information and Telecommunication Networks]. *Voprosy kiberbezopasnosti*, 2017, vol. 24, no. 5, pp. 72-82, doi: 10.21681/2311-3456-2017-5-72-82 (in Russian).

5. Maximov R. V., Pavlovskij A. V., Samohin V. F., Chernoles V. P. Informacionnaya bezopasnost' Rossii v sfere nauki i tekhniki [Information Security of Russia in Science and Technology]. *Informaciya i kosmos*, 2006, no. 4, pp. 94-102 (in Russian).

6. Maximov R. V., Sokolovskij S. P., Sharifullin S. R., Chernoles V. P. Innovacionnye informacionnye tekhnologii v kontekste obespecheniya nacional'noj bezopasnosti gosudarstva [Innovative Information Technologies in the Context of National Security]. *Innovacii*, 2018, vol. 233, no. 3, pp. 28-35 (in Russian).

7. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Survivability Assessment of Distributed Information and Telecommunication Networks. *Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017)*. Bauman Moscow Technical University, 2017, pp. 59-65 (in Russian).

8. The doctrine of information security of the Russian Federation. Decree of the President of the Russian Federation of December 5, 2016, no. 646. *Oficial'nyj internet-portal pravovoj informacii* [Official Internet portal of legal information]. Available at: http://publication.pravo.gov.ru/Document/View/0001201612060002 (accessed 01 September 2018) (in Russian).

9. Maximov R. V., Sokolovsky S. P., Gavrilov L. A. Hiding computer network proactive security tools unmasking features. *Selected Papers of the VIII All-Russian Conference with International Participation "Secure Information Technologies" (BIT 2017).* Bauman Moscow Technical University, 2017, pp. 88-92 (in Russian).

10. Vygovskij L. S., Maximov R. V. Model' prednamerennyh destruktivnyh vozdejstvij na informacionnuyu infrastrukturu integrirovannyh sistem svyazi [Model of Intentional Destructive Impacts on the Information Infrastructure of Integrated Communication Systems]. *Nauchno-tekhnicheskie vedomosti, St. Petersburg state Polytechnic University*, 2008, vol. 60, no. 3, pp. 166-173 (in Russian).

11. Vygovskij L. S., Maximov R. V. Model' prednamerennyh destruktivnyh vozdejstvij na informacionnuyu infrastrukturu integrirovannyh sistem svyazi [Model of Intentional Destructive Impacts on the Information Infrastructure of Integrated Communication Systems]. *Nauchno-tekhnicheskie vedomosti, St. Petersburg state Polytechnic University*, 2009, vol. 73, no. 1, pp. 181-187 (in Russian).

12. Maximov R. V., Savinov E. A. Ocenka zhivuchesti raspredelennyh integrirovannyh informacionnyh system. *Informacionnye tekhnologii i nanotekhnologii (ITNT-2016). Materialy Mezhdunarodnoj konferencii i molodezhnoj shkoly* [Information technologies and nanotechnologies (ITT-2016). Proceedings of the International conference and young scientists school]. Samara State Aerospace University (National Research University) named after academician S.P. Korolyov and Image Processing Systems Institute of RAS, 2016, pp. 431-438 (in Russian).

13. Maximov R. V., Aparin N. N., Astahov A. I., Zhirakovskij A. A., Ignatenko A. V., Kostyrev A. L., Nekhaev M. A. *Sposob sravnitel'noj ocenki struktur setej svyazi* [Method of Comparative Evaluation of Communication Network Structures]. Patent Russia, no. 2460123, 27.08.2012.

14. Maximov R. V., Ignatenko A. V., Kovalevskij S. G., Ozerov O. V., Tevs O. P., Shlyahtenko D. B. *Sposob sravnitel'noj ocenki struktur setej svyazi* [Method of Comparative Evaluation of Communication Network Structures]. Patent Russia, no. 2450338, 10.05.2012.

15. Maximov R. V., Berest P. A., Bogachev K. G., Vygovskij L. S., Ignatenko A. V., Kozhevnikov D. A., Krasnov V. A., Kuznecov V. E. *Sposob sravnitel'noj ocenki struktur informacionno-vychislitel'noj seti* [Method of Comparative Evaluation of Information and Computer Network Structures]. Patent Russia, no. 2408928, 10.01.2011.

16. Maximov R. V., Kozhevnikov D. A., Pavlovskij A. V. *Sposob zashchity vychislitel'noj seti (varianty)* [Method of Computer Network Protection (Variants)]. Patent Russia, no. 2325694, 27.05.2008.

17. Maximov R. V., Kozhevnikov D. A., Pavlovskij A. V., YUr'ev D. YU. *Sposob vybora bezopasnogo marshruta v seti svyazi (varianty)* [How to Select a Secure Route in the Communication Network (Options)]. Patent Russia, no. 2331158, 10.08.2008.

18. Maximov R. V., Andrienko A. A., Kozhevnikov D. A., Kolbasova G. S., Pavlovskij A. V., Starodubcev YU. I. *Sposob (varianty) i ustrojstvo (varianty) zashchity kanala svyazi vychislitel'noj seti* [Method (Options) and Device (Options) to Protect the Communication Channel of the Computer Network]. Patent Russia, no. 2306599, 20.09.2007.

19. Maximov R. V., Vetoshkin I. S., Drozd YU. A., Efimov A. A., Ignatenko A. V., Kozhevnikov D. A., Krasnov V. A., Kuznecov V. E. *Sposob zashchity vychislitel'noj seti s vydelennym serverom* [Method of Protection of a Computer Network with a Dedicated Server]. Patent Russia, no. 2449361, 10.02.2011.

20. Maximov R. V., Golub B. V., Goryachaya A. V., Kozhevnikov D. A., Lykov N. YU., Tihonov S. S. *Sposob maskirovaniya struktury seti svyazi* [A Method of Masking a Structure of a Communication Network]. Patent Russia, no. 2622842, 20.06.2017.

21. Maximov R. V., Iskol'nyj B. B., Lazarev A. A., Lykov N. YU., Horev G. A., Sharifullin S. R. *Sposob sravnitel'noj ocenki struktur setej svyazi* [Method of Comparative Evaluation of Communication Network Structures]. Patent Russia, no. 2626099, 21.07.2017.

22. Maximov R. V., Orekhov D. N., Proskuryakov I. S., Sokolovskij S. P. *Sposob zashchity vychislitel'nyh setej* [Method of Protection of Computer Networks]. Patent Russia, no. 2649789, 04.04.2018.

23. Dybko L. K., Ivanov I. I., Lykov N. YU., Maximov R. V., Proskuryakov I. S., Horev G. A., Sharifullin S. R. *Sposob maskirovaniya struktury seti svyazi* [A Method of Masking a Structure of a Communication Network]. Patent Russia, no. 2656839, 06.06.2018.

24. Golub B. V., Krasnov V. A., Lykov N. YU., Maximov R. V. *Sposob maskirovaniya struktury seti svyazi* [A Method of Masking a Structure of a Communication Network]. Patent Russia, no. 2645292, 19.02.2018.

25. Belov A. A., Ivanov I. I., Lazarev A. A., Maximov R. V., Miroshnichenko E. L., Sharifullin S. R. *Sposob maskirovaniya struktury seti svyazi* [A Method of Masking a Structure of a Communication Network]. Patent Russia, no. 2668979, 05.10.2018.

26. Bogovik A. V., Ignatov V. V. *EHffektivnost' sistem voennoj svyazi i metody ee ocenki* [Efficiency of Military Communication Systems and Methods of its Evaluation]. Saint Petersburg, Military Academy of Communications, 2006. 183 p. (in Russian).

27. Maximov R. V., Vygovskij L. S., Zargarov I. A., Kozhevnikov D. A., Pavlovskij A. V., Starodubcev Y. I., Hudajnazarov Y. K., Yurov I. A. *Sposob*

(varianty) zashchity vychislitel'nyh setej [Method (Options) of Protection of Computer Networks]. Patent Russia, no. 2307392, 27.09.2007.

28. Maximov R. V., Andrienko A. A., Kulikov O. E., Kostyrev A. L., Pavlovskij A. V., Lebedev A. YU. *Sposob kontrolya informacionnyh potokov v cifrovyh setyah svyazi* [Method of Control of Information Flows in Digital Communication Networks]. Patent Russia, no. 2267154, 27.12.2005.

29. Maximov R. V., Andrienko A. A., Kulikov O. E., Kostyrev A. L. *Sposob obnaruzheniya udalennyh atak na avtomatizirovannye sistemy upravleniya* [Method for Detecting Remote Attacks on Automated Control Systems]. Patent Russia, no. 2264649, 20.11.2005.

30. Maximov R. V., Ivanov I. I., Sharifullin S. R. Network Topology Masking in Distributed information Systems. *Selected Papers of the VIII all-Russian Conference with International Participation «Secure Information Technologies»*. Moscow, Bauman Moscow Technical University, 2017, pp. 83-87 (in Russian).

31. RFC 1191. Path MTU Discovery. Draft Standard. 1990. Available at: http://tools.ietf.org/html/rfc1191 (accessed 4 September 2018).

32. RFC 879. The TSP Maximum Segment Size and Related Topics. 1983. Available at: http://tools.ietf.org/html/rfc879#section-3 (accessed 6 September 2018).

33. Basaker R., Saati T. *Konechnye grafy i seti* [Finite Graphs and Networks]. Moscow, Nauka Publ., 1973. 38 p. (in Russian).

34. Kristofides N. *Teoriya grafov. Algoritmicheskij podhod* [Graph Theory: an Algorithmic Approach]. London, New York, Academic Press, 1975. 576 p.

35. Tanenbaum E., Uehzeroll D. *Komp'yuternye seti. Izdanie 5* [Computer network. Edition 5]. Saint-Petersburg, Piter Publ., 2017. 90 p. (in Russian).

36. RFC 791. DARPA internet program protocol specification. Enternet Standard. 1981. Available at: http://tools.ietf.org/html/rfc791 (accessed 06 September 2018).

Статья поступила 29 октября 2018 г.

Информация об авторах

Шерстобитов Роман Сергеевич – соискатель ученой степени кандидата технических наук. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E-mail: scherstobitov.rs@yandex.ru

Шарифуллин Сергей Равильевич – кандидат технических наук, доцент. Начальник кафедры. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E-mail: SharifullinSR@mail.ru

Максимов Роман Викторович – доктор технических наук, профессор. Профессор кафедры. Краснодарское высшее военное училище им. генерала ар-

мии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E-mail: rvmaxim@yandex.ru

Адрес: 350063, Россия, г. Краснодар, улица Красина, д. 4.

Masking of departmental-purpose integrated communication networks

R. S. Sherstobitov, S. R. Sharifullin, R. V. Maximov

Formulation of the problem*: in the conditions of information technologies development, integration of departmental-purpose communication networks and public ones, we need measures to protect integrated departmental-purpose communication networks against computer intelligence; these measures could form misconception about the structure of a departmental management system by controlling unmasking signs of information exchange. We can achieve the goal by implementing a masking exchange. However, due to the insufficient development of methodological and technological support for its implementation when using public communication networks, at present researchers have not got any solution for the task of hiding the fact of constructive traffic transmission and distortion of the hierarchy levels of communication nodes of the relevant management bodies (divisions) in integrated departmental-purpose communication networks.* ***The aim of the work*** *is to devise both a mathematical model for the synthesis of the network structure of masking exchanges and methods for implementing masking exchanges to increase the security of departmental-purpose integrated communication networks against computer intelligence.* ***The used methods****: there are two of them: the use of graph theory in the construction of minimum spanning trees by the criterion of the minimum intensity of information exchange between network nodes and the differentiation of routes between communication nodes by the safety criterion of transit communication nodes. They are the basis for the solution of the task of masking integrated departmental-purpose communication networks.* ***The scientific novelty*** *of the developed scientific and methodological apparatus consists in modifying the algorithms of minimum spanning trees, in applying them to solving the problem of synthesizing the network structure of a masking exchange, and in implementing a masking exchange when differentiating routes between communication nodes by the safety criterion of transit communication nodes.* ***The practical significance*** *of the developed scientific and methodological apparatus is to provide the possibility of distorting the algorithms of functioning of departmental-purpose integrated networks while protecting against computer intelligence according to specified requirements (in accordance with the cheating intent). It also results in, reducing the load of network subscribers by processing masking messages and ensuring timely delivery of messages when performing a masking exchange.* ***Result****: the use of the developed scientific and methodological apparatus allows us to implement a masking exchange to fulfill the idea of deception while reducing the load on network subscribers by processing masking messages and ensuring timely delivery of messages. The conducted simulation for a network of nine nodes shows that the transfer time of one Mbit of constructive traffic when entering terminator nodes decreases on average by 25% from the implementation of masking exchange without them.*

Keywords*: unmasking signs, communication network, masking exchange, minimum spanning tree, terminator node.*

Information about Authors

Roman Sergeevich Sherstobitov – Doctoral Student. The postgraduate student of the full-time state staff adjuncture. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security; synthesis and system analysis of information security systems of critical objects; masking and simulation of information resources of integrated departmental communication networks. E-mail: scherstobitov.rs@yandex.ru

Sergey Ravilievich Sharifullin – Ph.D. of Engineering Sciences, Associate Professor. Head of the Department. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security; synthesis and system analysis of information security systems of critical objects; masking and simulation of information resources of integrated departmental communication networks. E-mail: SharifullinSR@mail.ru

Roman Viktorovich Maximov – Dr. habil. of Engineering Sciences, Full Professor. Full Professor of the Department. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security, synthesis and system analysis of information security systems of critical objects, masking and simulation of information resources of integrated departmental communication networks. E-mail: rvmaxim@yandex.ru

Address: 350063, Russia, Krasnodar, Krasina street, 4.