На правах рукописи

Кушко Евгений Александрович

МЕТОД ЗАЩИТЫ ОТ СТОРОННЕГО ИССЛЕДОВАНИЯ ЛОКАЛЬНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ РЕКОНФИГУРАЦИИ ТОПОЛОГИИ СЕТЕВОГО УРОВНЯ

Специальность: 2.3.6 – методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Красноярск – 2025

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» (СибГУ им. ак. М.Ф. Решетнева)

Научный руководитель: кандидат технических наук, доцент
Золотарев Вячеслав Владимирович

Официальные оппоненты: **Максимова Елена Александровна**,
доктор технических наук, доцент,
МИРЭА – Российский технологический университет, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности»

Тебуева Фариза Биляловна,
доктор физико-математических наук, доцент, ФГАОУ ВО «Северо-Кавказский федеральный университет», профессор кафедры вычислительной математики и кибернетики факультета математики и компьютерных наук имени профессора Н.И. Червякова

Ведущая организация: ФГАОУ ВО «Южный федеральный университет»

Защита состоится «27» ноября 2025 г., в 15:15 на заседании диссертационного совета 24.2.415.04 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу: 634050, г. Томск, пр. Ленина, 40, каб. 201.

С диссертацией можно ознакомиться в библиотеке ТУСУР по адресу: 634045, г. Томск, ул. Красноармейская, 146, а также на сайте ТУСУР: https://postgraduate.tusur.ru/urls/n5eo1lgd

Автореферат разослан: «___»_____20__ г.

Ученый секретарь диссертационного совета — Костюченко Евгений Юрьевич

Общая характеристика работы

Актуальность темы исследования. Переход к активной защите в сфере информационной безопасности (ИБ) становится все более необходимым в связи с растущей сложностью и изощренностью угроз. Традиционные стратегии пассивной защиты, такие как, например, защита в глубину, уже недостаточны для борьбы с современными угрозами, особенно с APT-атаками (Advanced Persistent Threat) и эксплойтами «нулевого дня». Активная защита предполагает использование, помимо стандартных мер эшелонированной защиты, методы активного вовлечения и взаимодействия с злоумышленником, такие как технология информационного обмана (ИО) и технология защиты с использованием подвижных целей (MTD, Moving Target Defense).

Применяя эти методы, защитники могут обнаружить угрозы и нейтрализовать их до того, как они нанесут значительный ущерб. Это особенно важно для защиты от сложных многоэтапных атак, в которых учтены уязвимости и недостатки традиционных средств защиты информации (СЗИ). Эти методы в совокупности с автоматизацией еще больше повышают эффективность системы защиты, благодаря быстрому и адаптивному реагированию на возникающие угрозы. Меры, предлагаемые стратегиями активной защиты, позволяют защитникам минимизировать последствия его атак за счет динамичного и интеллектуального противодействия угрозам за счет противодействия на ранних стадиях реализации атаки.

Чем раньше защитники окажут противодействие злоумышленнику, тем с меньшими последствиями они столкнутся. Первой стадией реализации атаки является разведка. Противодействие на стадии разведки очень важно для ИБ, поскольку на этой стадии злоумышленник собирает важную информацию о целевой сети. Во время разведки злоумышленник выполняет исследование сети, а именно осуществляет: сканирование сети и портов, перехват и анализ сетевого трафика, сканирование уязвимостей. Полученные данные при исследовании сети используются для планирования точной и эффективной атаки. Пресекая или обманывая злоумышленника на стадии разведки, защитники могут предотвратить получение им информации, необходимой для осуществления атаки.

Совместное применение мониторинга в режиме реального времени, ИО, MTD и автоматического реагирования, вынуждают злоумышленника либо раскрыть себя, либо тратить больше ресурсов для того, чтобы дольше оставаться незамеченным в информационной системе (ИС). Раннее обнаружение и реагирование значительно снижает вероятность успешных атак, позволяя защитникам предотвратить их до того, как они перерастут в полномасштабные.

MTD играет особенно важную роль в противодействии исследованию ИС злоумышленником, внося непредсказуемость и адаптивность в среду. Во время разведки злоумышленник пытается составить карту сети и определить в ней цели для атаки. MTD противодействует этому, постоянно изменяя ключевые параметры сети: физические и логические адреса, номера портов,

маршруты передачи данных и другие. Это постоянное изменение сетевого окружения сбивает злоумышленника с толку, затрудняя сбор точной и долговременной информации и, таким образом, срывая проведение атаки. Динамически изменяя поверхность атаки, MTD заставляет злоумышленника тратить ресурсы на устаревшую или неверную информацию. Это не только нарушает планирование атаки, но и повышает вероятность обнаружения защитниками.

Проблемой защиты ИС от стороннего исследования при помощи технологий ИО и MTD занимаются в следующих зарубежных университетах: Центр коммуникационных исследований Канады (Канада, исследователи: Анни Де Монтини-Лебёф, Фредерик Масикот), Национальный университет оборонных технологий (Китай, исследователи: Гуйлинь Цай, Баошэн Ван, Вэй Ху, Тяньцзо Ван), Университет штата Канзас (США, исследователи: Скотт Делоач, Руй Чжуан и Синьмин Оу), Университет штата Северная Каролина (США, исследователи: Гарри Перрос), Варшавский университет технологий (Польша, исследователи: Лукаш Яловский, Марек Змуда, Мариуш Равский), Неаполитанский университет имени Федерико II (Италия, исследователи: Валентина Казола и Алессандра Де Бенедиктис), Технологический институт Флориды (США, исследователи: Марко Карвальо и Ричард Форд) и других; а также в научно-исследовательских лабораториях крупных IT-компаний: Cisco Systems (США, исследователи: Панос Кампанакис и Цегереда Бейене), Symantec Corpotation (США, исследователи: Су Чжан) и других.

В Российской Федерации данную проблему исследуют в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича (Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. и др.), в Краснодарском высшем военном училище им. генерала армии С.М. Штеменко (Ворончихин И. С., Иванов И. И., Максимов Р. В., Соколовский С. П. и др.), в Кубанском государственном технологическом университете (Макарян А. С. и др.), в Военной академии связи им. Маршала Советского Союза С .М. Буденного (Спицын О.Л. и др.) и в других университетах и организациях.

Существующие решения MTD для защиты локальных сетей передачи данных обычно оперируют ограниченным набором параметров, например, такими как IP-адреса, порты и маршруты, причем очень часто в действительности оставляя их статичными, лишь подменяя их фиктивными значениями, которые злоумышленник, выявив некоторые закономерности, может установить. Хотя эти изменения обеспечивают определенный уровень защищенности, сбивая злоумышленника с толку во время исследования сети, такая узкая направленность этих решений потенциально оставляет сеть уязвимой. Изменяя или подменяя некоторый ограниченный набор параметров, MTD не может в полной мере предотвратить сложные атаки. Злоумышленник может выявить закономерности или слабые места в инфраструктуре, на которые MTD никак не влияет.

Еще одним ограничением существующих решений MTD является отсутствие активных контрмер, позволяющих без участия защитников изолиро-

вать или нейтрализовать злоумышленника. Существующие решения MTD в основном сосредоточены на том, чтобы сделать сеть динамичной, и полагаются на то, что в результате этих изменений злоумышленник воспользуется устаревшей или ложной информацией и тем самым демаскирует себя. Эти решения не позволяют в автоматическом режиме блокировать злоумышленника после его обнаружения, а полагаются на ручные действия защитников. В результате злоумышленник имеет возможность продолжать исследование сети до тех пор, пока защитники не примут соответствующие меры по его нейтрализации.

В соответствии с текущим состоянием в предметной области, автором предложен метод защиты локальной сети передачи данных от стороннего исследования на основе реконфигурации топологии сетевого уровня. Учитывая ранее изложенные факты, разработка таких решений является актуальной научно-технической задачей. Для того, чтобы быть эффективным с точки зрения ИБ, предлагаемый метод должен удовлетворять следующим требованиям: динамическое распределение адресов; динамическая реконфигурация топологии сети; случайная маршрутизация; обнаружение и реагирование на исследование сети; автоматизированное восстановление и реконфигурация.

Реализация этих требований позволит защитить локальную сеть передачи данных от исследования злоумышленником, так как сетевая среда становится непредсказуемой и сложной, а злоумышленник может быть автоматически изолирован в случае обнаружения.

Целью диссертационного исследования является повышение защищенности локальной сети передачи данных от стороннего исследования за счет изменения поверхности атаки.

Для достижения поставленной цели необходимо решить **следующие задачи**:

1. Разработать модифицированный итерационный метод реконфигурации топологии сетевого уровня. Действие метода должно быть направлено на ограничение времени актуальности информации об адресах, топологии и маршрутизации локальной сети передачи данных, изменяя поверхность атаки.

2. Разработать модифицированную математическую модель, которая отражает действие предложенного метода и предназначена для оценки критичного периода реконфигурации и оценки защищенности как вероятность идентификации целевого хоста при каждой итерации метода.

3. Разработать новый алгоритм формирования топологии сетевого уровня и реализующее его программное средство в соответствии с предложенным методом, а также оценить их эффективность.

Объектом исследования является технология защиты с использованием подвижных целей. **Предметом исследования** являются методы и средства реконфигурации топологии локальной проводной стационарной сети. **Основными методами исследования** являются методы системного анализа, теории информации, теории графов и теории защиты информации. Использо-

вались имитационный и лабораторный типы экспериментов для всестороннего изучения предложенного метода.

Научная новизна результатов работы и проведенных исследований:

1. Предложен модифицированный итерационный метод для защиты локальной сети передачи данных от стороннего исследования, отличающийся от существующих подходом к созданию подвижных целей, основанном на перегруппировке хостов в сочетании с рандомизацией адресов и маршрутов.

2. Предложена модифицированная математическая модель оценки защищенности предложенного метода, основанного на технологии MTD, отличающаяся от существующих способом оценки защищенности через вероятность идентификации целевого хоста при каждой итерации метода.

3. Предложен новый алгоритм формирования топологии сетевого уровня и реализующее его программное средство, предназначенные для защиты от исследования злоумышленником локальной сети передачи данных, отличающиеся от существующих способом создания отношений между хостами сети.

Значение для теории состоит в развитии методов и моделей обеспечения защиты локальной сети передачи данных от исследования злоумышленником.

Практическая ценность работы заключается в расширении способов использования технологий локальной сети передачи данных для повышения уровня их защищенности.

Достоверность работы подтверждается теоретическими и практическими результатами, полученными с использованием предложенного метода, и их сопоставлением с имеющимися современными теоретическими и экспериментальными данными, полученными другими авторами в этой области.

Положения, выносимые на защиту:

1. Модифицированный итерационный метод защиты от стороннего исследования локальной сети передачи данных на основе реконфигурации топологии сетевого уровня, позволяющий изменить поверхность атаки до состояния, при котором множество хостов, идентифицированных злоумышленником, соответствует пустому множеству при каждой его итерации.

Соответствует пункту 6 паспорта специальности 2.3.6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

2. Предложена модифицированная математическая модель оценки защищенности сети, формируемой на основе предложенного метода, при помощи которой установлено, что вероятность идентификации целевого хоста на каждой итерации метода составляет $1/N$, где N – количество хостов сети, в отличие от статичной сети, где вероятность в процессе её исследования стремится к 1.

Соответствует пункту 10 паспорта специальности 2.3.6. Модели и методы оценки защищенности информации и информационной безопасности объекта.

3. Предложен новый алгоритм формирования топологии сетевого уровня и реализующее его программное средство, предназначенные для защиты от исследования злоумышленником локальной сети передачи данных, позволяющие на каждой итерации изменить поверхность атаки и свести вероятность идентификации целевого хоста к $1/N$, где N – количество хостов сети.

Соответствует пункту 6 паспорта специальности 2.3.6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

Апробация работы. Основные положения и результаты работы прошли всестороннюю апробацию на семинарах кафедры безопасности информационных технологий СибГУ им. М. Ф. Решетнева, на семинарах факультета безопасности ТУСУР, а также на конференциях:

1. II Международная научно-практическая конференция, посвященная Дню космонавтики, «Актуальные проблемы авиации и космонавтики», г. Красноярск, 11–15 апреля 2016;
2. XVII Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности «SIBINFO – 2017», г. Томск, 19–20 апреля 2017;
3. IV Международная научно-практическая конференция, посвященная Дню космонавтики, «Актуальные проблемы авиации и космонавтики», г. Красноярск, 9–13 апреля 2018;
4. XXII Международная научно-практическая конференция, посвященная памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева «Решетневские чтения», г. Красноярск, 12–16 ноября 2018;
5. V Международная научно-практическая конференция, посвященная Дню космонавтики, «Актуальные проблемы авиации и космонавтики», г. Красноярск, 8–12 апреля 2019;
6. Международная научно-техническая конференция «Автоматизация» (RusAutoCon), г. Сочи, 8–14 сентября 2019;
7. I Международная конференция APITECH-I 2019: Прикладная физика, информационные технологии и инжиниринг, г. Красноярск, 25–27 сентября 2019;
8. VI Международная научно-практической конференция, посвященная Дню космонавтики, «Актуальные проблемы авиации и космонавтики», г. Красноярск, 13–17 апреля 2020;
9. II Международная конференция MIP: Engineering-II 2020: Модернизация, Инновации, Прогресс: Передовые технологии в материаловедении, машиностроении и автоматизации, г. Красноярск, 16–18 апреля 2020;
10. XXIV Международная научно-практическая конференция, посвященная памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева «Решетневские чтения», г. Красноярск, 10–13 ноября 2020;

11. VII Международная научно-практическая конференция, посвященная Дню космонавтики, «Актуальные проблемы авиации и космонавтики», г. Красноярск, 12–16 апреля 2021;

12. III Международная научная конференция MIP Engineering-III 2021: Модернизация, Инновации, Прогресс: Передовые технологии в материаловедении, машиностроении и автоматизации, г. Красноярск, 29–30 апреля 2021;

13. Межвузовская научно-теоретическая конференция в рамках Сибирского форума «Информационная безопасность – 2021», г. Новосибирск, 29 ноября – 5 декабря 2021;

14. VIII Международная научно-практическая конференция, посвященная Дню космонавтики, «Актуальные проблемы авиации и космонавтики», г. Красноярск, 11–15 апреля 2022.

15. II Межвузовская научная школа-семинар «Современные тенденции развития методов и технологий защиты информации», г. Москва, 18–21 октября 2022.

Реализация результатов работы. Результаты работы были внедрены и использованы в АО «НПП «Радиосвязь» на имитационном стенде станции наземной связи для исследования применимости технологии MTD для защиты от стороннего исследования её сети управления, а также в образовательный процесс университета СибГУ им. М. Ф. Решетнева для студентов кафедры безопасности информационных технологий.

Диссертационная работа выполнена автором единолично в рамках выполнения проекта Грант ИБ № 40469-07/2021-К «Метод реализации защищенного обмена данными на основе динамической топологии сети», 2021–2022 гг.

Публикации по теме диссертации. По теме исследования опубликовано 20 печатных работ, из них 5 статей в журналах перечня ВАК РФ и 5 – в изданиях, индексируемых в международных базах цитирования Web of Science и/или Scopus.

Личный вклад. Все результаты, изложенные в диссертации, получены автором самостоятельно. Постановка цели и задач, обсуждение планов исследований и полученных результатов выполнены автором совместно с научным руководителем.

Структура и объем работы. Диссертационное исследование объемом 206 страниц состоит из оглавления, введения, основной части, состоящей из трех глав, заключения, библиографического списка из 136 цитируемых источников и списка сокращений, 5 приложений, а также 34 рисунков и 10 таблиц.

Основные положения работы

Во введении обосновывается актуальность темы диссертации, формулируются цель и задачи исследования, обсуждаются научная новизна и практическая ценность выносимых на защиту результатов.

Первая глава посвящена проблеме защиты локальных сетей передачи данных от стороннего исследования. В главе проведен анализ стратегий ИБ. Основной недостаток стратегий пассивной защиты в сравнении с стратегиями активной защиты заключается в их статичности. Стратегии пассивной защиты опираются на заранее определенные эшелоны, которые остаются неизменными, что делает ИС уязвимой, так как злоумышленник может использовать известные уязвимости и обойти эти эшелоны. Стратегии активной защиты предлагают использование, помимо стандартных мер эшелонированной защиты, методы активного вовлечения и взаимодействия с злоумышленником, такие как технология информационного обмана (ИО) и технология защиты с использованием подвижных целей (MTD, Moving Target Defense). Эти методы позволяют эффективнее реагировать на атаки и нейтрализовать их на ранних стадиях, обеспечивая более надежную защиту в условиях современных угроз.

Далее в главе проанализированы существующие меры активной защиты. Они нацелены на нейтрализацию злоумышленника на ранних стадиях атаки, так как это имеет важное значение для минимизации потенциального ущерба и предотвращения дальнейшего проведения атаки. Пресекая действия злоумышленника на ранней стадии, защитники могут предотвратить эскалацию и более эффективно сдерживать угрозу. Такой упреждающий подход не только снижает последствия атаки, но и позволяет получить ценные сведения о тактиках и инструментах злоумышленника, которые можно использовать для защиты от будущих угроз.

Защитники после реализации базовых мер активной защиты могут повысить уровень ИБ при помощи MTD и ИО. MTD повышает ИБ, постоянно изменяя поверхность атаки, например, изменяя параметры ИС, ПО или сети. Это затрудняет злоумышленнику поиск целей и уязвимостей, таким образом нейтрализуя его до того, как он успеет развить атаку. В сочетании с ИО, который использует ложные компоненты для введения злоумышленника в заблуждение, MTD создает динамичную систему защиты, которая значительно повышает шансы остановить атаку на начальных этапах.

В результате анализа текущего положения в области MTD, сделан вывод о том, что существующие решения MTD имеют ряд ограничений, поэтому существует необходимость в разработке более совершенных решений MTD. Несмотря на это, текущие разработки показывают перспективность применения MTD.

В заключении главы обоснована актуальность исследования, цель, поставленные задачи и необходимость создания метода защиты от стороннего исследования локальной сети передачи данных на основе реконфигурации топологии сетевого уровня.

Во второй главе приведены описание объекта защиты, потенциальных угроз, модель нарушителя, алгоритмическое обеспечение предложенного метода и описание его программной реализации. В работе рассматривается объект защиты со следующими характеристиками:

1. Сегмент локальной сети передачи данных, в котором обрабатывается конфиденциальная информация.

2. Изначальная топология этого сегмента – это звезда или дерево.

3. Сеть построена на технологиях Transmission Control Protocol / Internet Protocol (TCP/IP).

4. В работе не учитываются аспекты беспроводных сетей, а рассматривается только стационарная локальная проводная сеть Ethernet.

5. В сети не происходит изменений на физических и канальных уровнях в рамках структурной взаимосвязи хостов.

6. Хосты в сети неотличимы друг от друга с точки зрения работающих на них сетевых сервисом и служб.

7. В случае, если злоумышленник был обнаружен, он может быть изолирован, в следствие чего он не сможет перемещаться по сети и осуществлять её исследование.

Информация об объекте, подлежащая защите:

1. Топология сетевого уровня: физические адреса (MAC), логические адреса (IP), маршруты передачи данных, логическая топология.

2. Данные о взаимодействии на сетевом уровне: паттерны взаимодействия между хостами, статистические данные о взаимодействии, роль и назначение каждого хоста в сети.

Эта информация служит основой для планирования злоумышленником более сложных атак. Защита этой информации имеет важное значение для создания безопасной и устойчивой сетевой инфраструктуры, а противодействие сбору этой информации злоумышленником может предотвратить реализацию всей атаки.

Таким образом, в качестве потенциальных рассматриваются угрозы, касающиеся исследования сети злоумышленником, а именно следующие угрозы из банка данных угроз ФСТЭК: УБИ.099, УБИ.098, УБИ.104, УБИ.116, УБИ.103, УБИ.132. Актуальность этих угроз подтверждается публичными аналитическими отчетами и публикациями ведущих компаний и исследователей в области ИБ.

В работе рассматривается злоумышленник, который:

1. сосредоточился исключительно на исследовании сети, не прибегая к деструктивным действиям;

2. действует изнутри сети, собирая информацию о ней;

3. может перемещаться по сети, исследуя её;

4. не имеет никаких предварительных знаний о сети.

С точки зрения планируемых контрмер, предлагаемый метод является модификацией класса методов технологии MTD, направленных на изменения топологии сети (рисунок 1).

Цель предлагаемого метода – защита локальной сети передачи данных от стороннего исследования при помощи периодического изменения топологии (далее – реконфигурации). На рисунке зеленым выделена модификация относительно оригинального метода.

Модификация предполагает генерацию новой топологии на основе групп в сочетании с изменением физических и логических адресов хостов сети, а также маршрутов передачи информации (далее – топологии сетевого уровня). Таким образом, топология сетевого уровня – это набор параметров сети, который включает в себя: физический и логический адреса, маршруты передачи данных и логическую топологию сети.

Генерация новой топологии заключается в следующем. Хосты случайно и равномерно разбиваются на группы. Количество групп выбирается случайно из диапазона от 2 до $N - 1$, где N – количество хостов сети. Из общего адресного пространства метода для каждой группы выделяется свое случайное подпространство. Из адресного подпространства группы случайным образом выдаются физические и логические адреса участникам этих групп.

Затем эти группы последовательно-случайно соединяются между собой. Затем на основе полученной топологии генерируются маршруты. Таким образом получается новая топология. При этом при формировании новой топологии из взаимодействия могут быть исключены потенциально опасные хостыы, которые представляют из себя угрозу. Изменение топологии может быть инициировано истечением временного периода, оповещением от других СЗИ, а также по обнаружению злоумышленника в результате мониторинга сети.

Модифицированный метод в отличие от оригинального предусматривает изменения не только топологии сети, но и случайные изменения физических и логических адресов (методы, направленные на изменения адресов и портов), а также случайные изменения маршрутов (методы, направленные на изменения маршрутов).

Случайное разделение хостов на группы и назначение случайных физических и логических адресов вносит значительную неопределенность для злоумышленника. Эта непредсказуемость затрудняет составление карты сети и определение целей, нарушая стадию разведки.

Благодаря последовательному соединению групп в случайном порядке и динамическому генерированию новых маршрутов сеть постоянно изменяется. Это затрудняет злоумышленнику использование ранее собранной информации, вынуждая его начинать разведку заново при каждом изменении.

Далее приведена оценка вероятности идентификации целевого хоста при помощи математической модели. В качестве основы для математической модели взята математическая модель информационной сети на основе теории графов. Основная её модификация заключается в изменении взаимосвязей между хостами в течение времени.

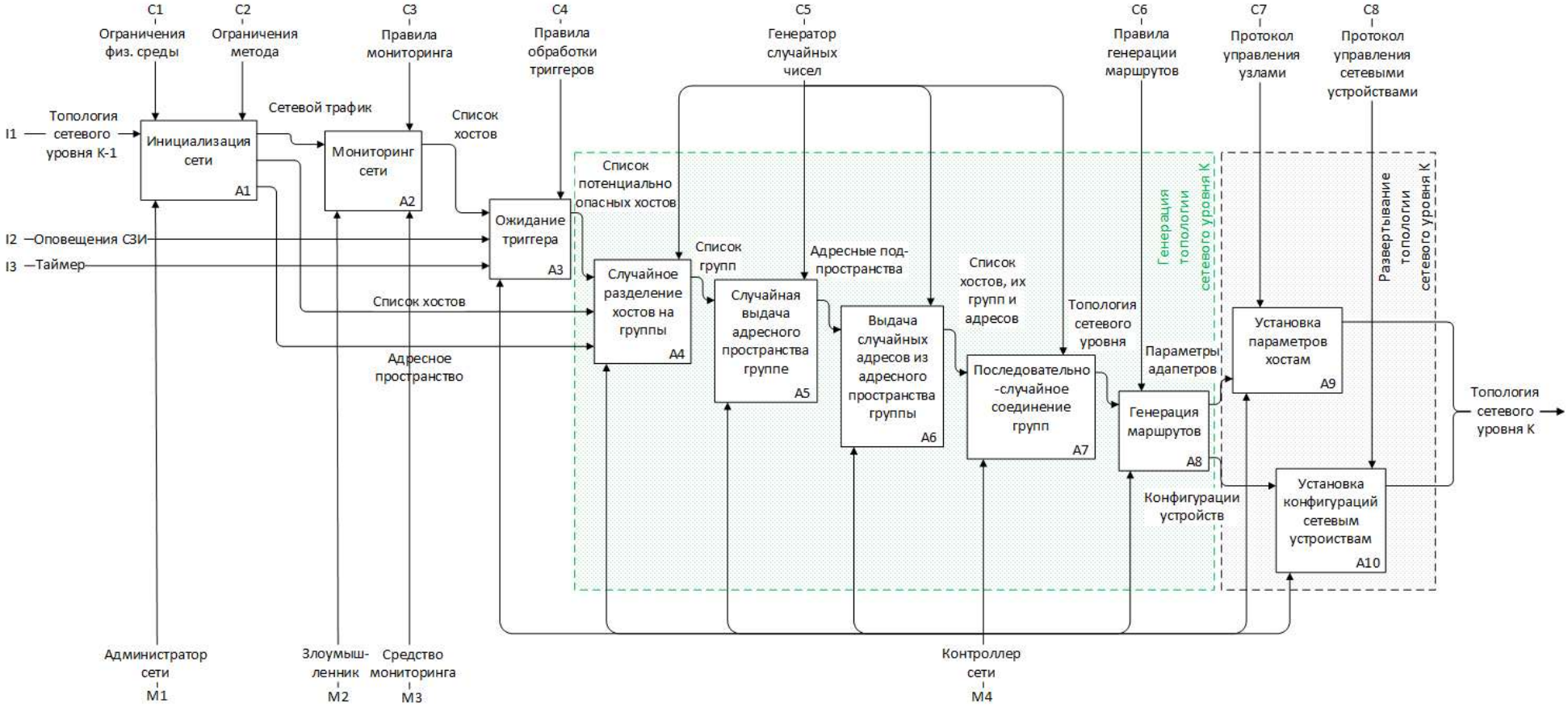

Рисунок 1 – IDEF0-диаграмма предлагаемого метода

Целевой хост – это компьютер, сервер или другое оконечное устройство сети, которое злоумышленник выбирает в качестве объекта для взлома, эксплуатации уязвимостей, проведения вредоносных действий или, иначе говоря, достижения своей цели. Злоумышленник проводит исследование сети, чтобы выбрать целевой хост.

Пусть существует некоторая локальная сеть передачи данных, объединяющая внутри себя N устройств. Тогда логический уровень данной сети можно представить в виде множества вершин V мощностью N. С момента начала эксперимента в начале каждой итерации реконфигурации будут выполняться следующие действия:

1. Случайным равновероятным образом выбирается число групп разбиения M, принадлежащее промежутку от 2 до N включительно. Следует также отметить, что на протяжении всего эксперимента для выбора случайного элемента используется равномерное распределение.

2. Все вершины из множества V разделяются на M множеств S_i.

3. Каждое множество S_i $(i = 1, \dots, M)$ дополняется ребрами E_{S_i} таким образом, чтобы получить граф-звезду $G_{S_i}(S_i, E_{S_i})$. Обозначим те вершины, степень которой больше 1 – центральными (или центрами), остальные вершины – крайними. Отметим, что центральная вершина в каждом множестве S_i выбирается случайным образом.

4. Составляется граф $G(V, E)$, получаемый при помощи объединения графов G_{S_i} путем соединения их между собой при помощи множества дополнительных ребер $e_i^{'}$ таким образом, что ребро $e_i^{'}$ связывает центральную вершину графа G_{S_i} с центральной вершиной графа $G_{S_{i+1}}$.

Для того, чтобы отразить процессы передачи информации между вершинами графа G, введем множество $W = \{w_i\}$ направленных каналов передачи информации между вершинами, каждый элемент которого представляет из себя последовательное множество вершин, через которые проходит кратчайший маршрут от одного заранее заданного хоста к другому (включая начальный и конечный хост). Следует также отметить, что в силу особенностей строения графа G, каждой паре вершин (v_i, v_j) будет соответствовать единственный маршрут во множестве W.

Таким образом, граф сети представляет из себя граф (1):

$$G(V, E) = \bigcup_i^M G_i \cup \bigcup_i^{M-1} e_i', \quad (1)$$

где $G_i(V_i, E_i)$ – множество графов-звезд,

e_i' – дополнительные ребра, соединяющие внутренние вершины графов G_i.

Данная модель подвергается атаке со стороны злоумышленника, включающей в себя две возможные глобальные стратегии: сканирование, пассивный перехват и анализ сетевого трафика.

При стратегии сканирования злоумышленник последовательно перебирает адреса в сети, при этом его основные затраты по времени складываются

из времени на идентификацию того, соответствует ли адрес в сети функционирующему хосту и на анализ того, является ли этот хост целевым для атаки. В таком случае среднее время на компрометацию сети будет:

$$t_{\text{оп.опт.}} = 0.5\left(N \cdot t_{\text{ид.}} + N_{\text{адр}} \cdot t_{\text{ска.}}\right) \quad 2)$$

где N – количество хостов в сети

$t_{\text{ид.}}$ – время, требуемое злоумышленнику на реализацию одной попытки идентификации хоста;

$t_{\text{ска.}}$ – время одного сканирования одного адреса;

$N_{\text{адр}}$ – количество адресов в сети.

А период реконфигурации будет задаваться как (7):

$$\tau_{\text{р.}} = p_{\text{кр.}}\left(N \cdot t_{\text{ид.}} + N_{\text{адр}} \cdot t_{\text{ска.}}\right) \quad (3)$$

где $p_{\text{кр.}}$ – верхняя границу вероятности обнаружения целевого хоста.

При пассивном анализе сети злоумышленник перехватывает трафик, проходящий через определенный хост, получая возможности при помощи анализа сообщений получать информацию о том, каким адресам в сети соответствуют функционирующие устройства. Таким образом, чтобы скомпрометировать систему, необходимо, чтобы злоумышленник узнал адрес целевого хоста, что достигается в том случае, если:

1. Злоумышленник выбрал вершину для перехвата таким образом, чтобы существовал хотя бы один маршрут w_i, такой чтобы ему принадлежали и целевая вершина и вершина, трафик которой перехватывается. Вероятность этого события описывается следующими формулами (4-6):

$$P_1 = N_{\text{и}}/N, \quad (4)$$

где $N_{\text{и}}$ – среднее число известных злоумышленнику вершин;

N – общее количество вершин в графе сети.

$$N_{\text{и}} = \frac{1}{N}\sum_{v_i \in V} |V_{\text{зл.}}(v_i)| \quad (5)$$

где $V_{\text{зл.}}$– множество известных злоумышленнику вершин;

$$V_{\text{зл.}} = \{x \in w_i : v_{\text{зр.}} \in w_i, w_i \in W\} \quad (6)$$

2. Злоумышленник из всех известных ему вершин смог выбрать ту, которая соответствует целевому хосту, вероятность чего (7):

$$P_2 = 1/N_{\text{и}} \quad (7)$$

Таким образом общая вероятность компрометации сети в таком случае (8):

$$P_{\text{к}} = P_1 \cdot P_2 = \frac{N_{\text{и}}}{N} \cdot \frac{1}{N_{\text{и}}} = \frac{1}{N} \quad (8)$$

Для данной модели характерны следующие ограничения, а именно предполагается, что:

1. Целевой хост не отличим от остальных без приложения дополнительных затрат на идентификацию (поведение и расположение хостов не дает злоумышленнику никакой дополнительной информации).

2. При стратегии сканирования затраты злоумышленника на сканирование и идентификацию каждого хоста в сети одинаковы и равны $t_{\text{ска.}}$ и $t_{\text{ид.}}$.

3. Злоумышленник может принять любой хост за целевой с одинаковой вероятностью.

4. Все хосты отправляют пакеты с одной и той же частотой, равной $\nu = 1/\tau$ сообщений в секунду, равновероятно любому потенциальному получателю в соответствии с множеством W.

5. При перехвате сообщения, оно содержит информацию как об хостах получателе и отправителе, так и о следующем шлюзе.

6. Пакеты доставляются мгновенно, а также то, что пропускной способностью каналов передачи информации в данной задаче можно пренебречь.

7. Группы распределены по адресному пространству в сети равномерно, а участники групп распределены равномерно по адресному пространству своих групп.

8. Злоумышленник использует все ресурсы хоста, в который он внедрился, для исследования сети.

Основной характеристикой, влияющей на защищенность сети как при пассивном перехвате и анализе, так и при сканировании, является мощность множества V. Проведем более подробный анализ на примере стратегии сканирования сети и оценим критичный период реконфигурации топологии сетевого уровня $\tau_{\text{кр.}}$.

Для того, чтобы оценить период реконфигурации, необходимо определить время $t_{\text{зл.}}$, за который злоумышленник сможет собрать всю информацию о локальной сети передачи данных. Модель анализа локальной сети передачи данных злоумышленником состоит из следующих шагов.

Начало отсчета времени совпадает с моментом «внедрения» злоумышленника в хост.

Каждый хост v_i один раз в определенный период времени τ отправляет пакет данных равновероятно по одному из заранее определенных каналов связи.

При попадании пакета данных, содержащего информацию о «незараженной» вершине, к злоумышленнику, он будет вынужден потратить время обработки $t_{\text{обр.}}$ на каждую новую вершину, о которой он узнает из пакета данных.

Пока злоумышленник обрабатывает один пакет данных, он не может начать обрабатывать следующий, но может сохранять их для последующей обработки. Также злоумышленник не тратит время для обработки уже выявленного адреса.

Введем функцию $\rho(v_i)$, которая означает вероятность того, что пакет данных, содержащий информацию о вершине v_i попадет в «зараженную» вершину при рассылке пакетов. В таком случае среднее количество пакетов,

за которое информация о вершине v_i попадет в «зараженную» вершину равна $1/\rho(v_i)$, при этом $\rho(v_i)$ составляет (9):

$$\rho(v_i) = 1 - \prod_{v_j \in V} \left(1 - \frac{\alpha(v_j, v_i)}{\beta(v_j)}\right), \tag{9}$$

где $\beta(v_j)$ – количество маршрутов из вершины v_j;

$\alpha(v_j, v_i)$ – количество маршрутов из вершины v_j, включающих в себя вершину v_i.

Пусть $t_1, t_2, \ldots, t_n$ – неубывающая последовательность, где t_i – среднее время ожидания, за которое злоумышленник будет узнавать об определенной вершине. Тогда можно задать рекуррентно последовательность моментов времени, во время которых злоумышленник будет узнавать о новых хостах.

Пусть F_i – момент времени, в который злоумышленник получит информацию об i-том хосте, $ReLU(x)$ – Rectified Linear Unit (выпрямленная линейная функция). Тогда получим следующий набор (10).

$$\begin{gathered} F_1 = t_1 + t_{\text{обр.}}, \\ F_2 = F_1 + ReLU(t_2 - F_1) + t_{\text{обр.}}, \\ \vdots \\ F_i = F_{i-1} + ReLU(t_i - F_{i-1}) + t_{\text{обр.}} \end{gathered} \tag{10}$$

Таким образом, при заданном графе $G(V, E)$ и множестве маршрутов передачи сообщений W можно построить график получения злоумышленником информации о существующих вершинах и в соответствии с ним (принимая $F_{N_и} = \tau_{\text{кр.}}$) произвести оценку критичного периода реконфигурации топологии сетевого уровня.

Таким образом, предложенный метод изменяет поверхность атаки с точки зрения злоумышленника. Поверхность атаки – это совокупность «точек взаимодействия» с ИС, сетью или приложением. Применительно для сети – это совокупность открытых портов, IP-адресов, протоколов, сетевых интерфейсов и других компонентов, доступных для взаимодействия. Злоумышленник при помощи исследования сети изучает доступную ему поверхность атаки, а предложенный метод изменяет её при помощи реконфигурации топологии сетевого уровня. Поверхность атаки изменяется из-за того, что собранные ранее данные утратили свою актуальность – «точки взаимодействия» стали располагаться в других сегментах сети по новым адресам.

Далее в главе приведен алгоритм формирования топологии сетевого уровня (рисунок 2). Сеть управляется централизованно участником-сервером, и алгоритм формирования топологии сетевого уровня выполняется им же. Участник-сервер, в соответствии с предложенным методом, во время своего функционирования постоянно ожидает следующие события:

1. оповещения;
2. истечение временного периода реконфигурации.

На некоторых из участников взаимодействия расположены средства обнаружения вторжений. Когда злоумышленник использует активное сканиро-

вание для исследования сети, то участник взаимодействия детектирует такое событие и оповещает об этом участника-сервера. Таким образом происходит реконфигурация топологии сетевого уровня. Реконфигурация также может быть инициирована оповещениями от других СЗИ. Реконфигурация также инициируется по истечению таймера. Период фиксированный и может быть задан администратором сети MTD.

Во время своего функционирования участник-сервер периодически посылает запросы участникам взаимодействия об их текущем статусе, чтобы удостовериться в том, что участник взаимодействия находится в сети и готов принимать новые конфигурации. Для того, чтобы сеть MTD функционировала, должно быть, как минимум, два участника взаимодействия.

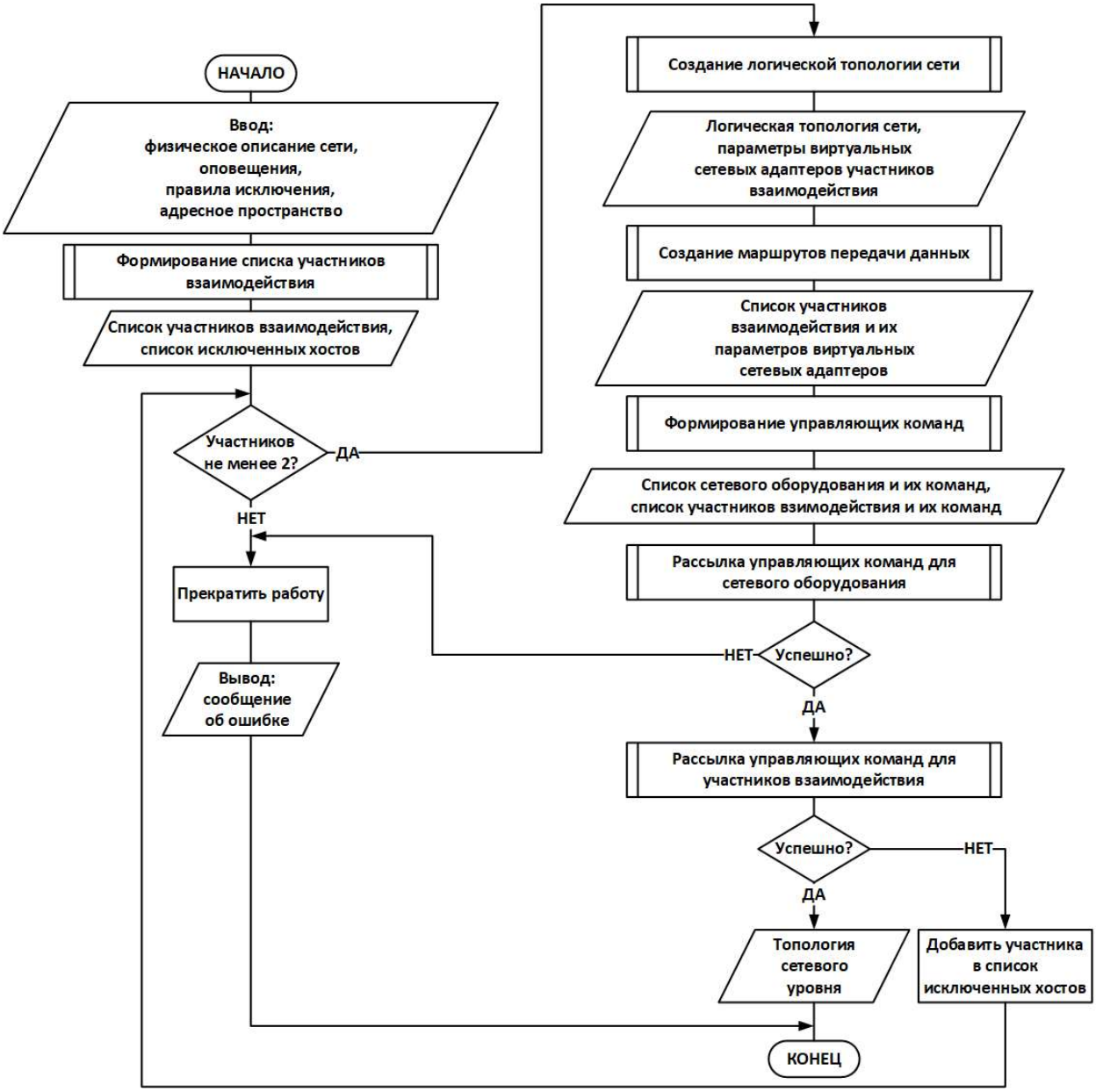

Рисунок 2 – Алгоритм формирования топологии сетевого уровня

В случае обнаружения сканирования участников взаимодействия, участник-сервер принимает оповещения от них, которые содержат в себе информацию о сканирующем хосте. При помощи этих оповещений участник-сервер формирует список потенциально опасных хостов. К потенциально опасным хостам могут быть применены определенные меры согласно заданным правилам исключения.

На основе списков подключенных участников взаимодействия и потенциально опасных хостов, правил исключения, физическом описании сети и доступном адресном пространстве участник-сервер сначала формирует топологию сетевого уровня.

Алгоритм формирования топологии сетевого уровня состоит из следующих важных компонентов:

1. формирование списка участников взаимодействия;
2. создание логической топологии сети;
3. создание маршрутов передачи данных;
4. формирование управляющих команд;
5. рассылка управляющих команд.

Формирование списка участников взаимодействия происходит следующим образом. Сначала выбирается хост из физического описания сети, который должен быть включен во взаимодействие. Физическое описание сети создает администратор сети MTD и предоставляет его участнику-серверу. Далее этот хост проверяется на присутствие в списке потенциально опасных хостов. В случае, если участник взаимодействия является потенциально опасным хостом, он может быть исключен из взаимодействия в соответствии с правилами исключения, которые задает администратор сети MTD.

Если хост в сети, то есть он присутствует в физическом описании, достижим для участника-сервера и готов принимать конфигурации, то этот хост добавляется в список участников взаимодействия. Затем рассматривается следующий хост из физического описания сети и так далее.

Так как алгоритм создания списка участников представляет собой последовательный проход физического описания сети, его сложность будет составлять $O(n)$.

Хост может быть исключен из взаимодействия следующими способами:

1. отключен от локальной сети;
2. перемещен в отдельную изолированную подсеть, например, для дальнейшего изучения его поведения.

Кроме того, хост может быть исключен:

1. на определенное время, т.е. хост может быть включен как участник взаимодействия через истечение заданного временного периода;
2. навсегда.

На рисунке 2 представлен алгоритм создания логической топологии сети. Логическая топология сети строится путем деления участников взаимодействия на группы. Каждая группа образует выделенную подсеть. Внутри каждой группы один участник взаимодействия выбирается в качестве внут-

реннего участника-шлюза. Соответственно, весь трафик группы, к которой выбранный внутренний участник-шлюз принадлежит, будет проходить через него. Внутренний участник-шлюз выбирается случайным образом при каждой новой реконфигурации.

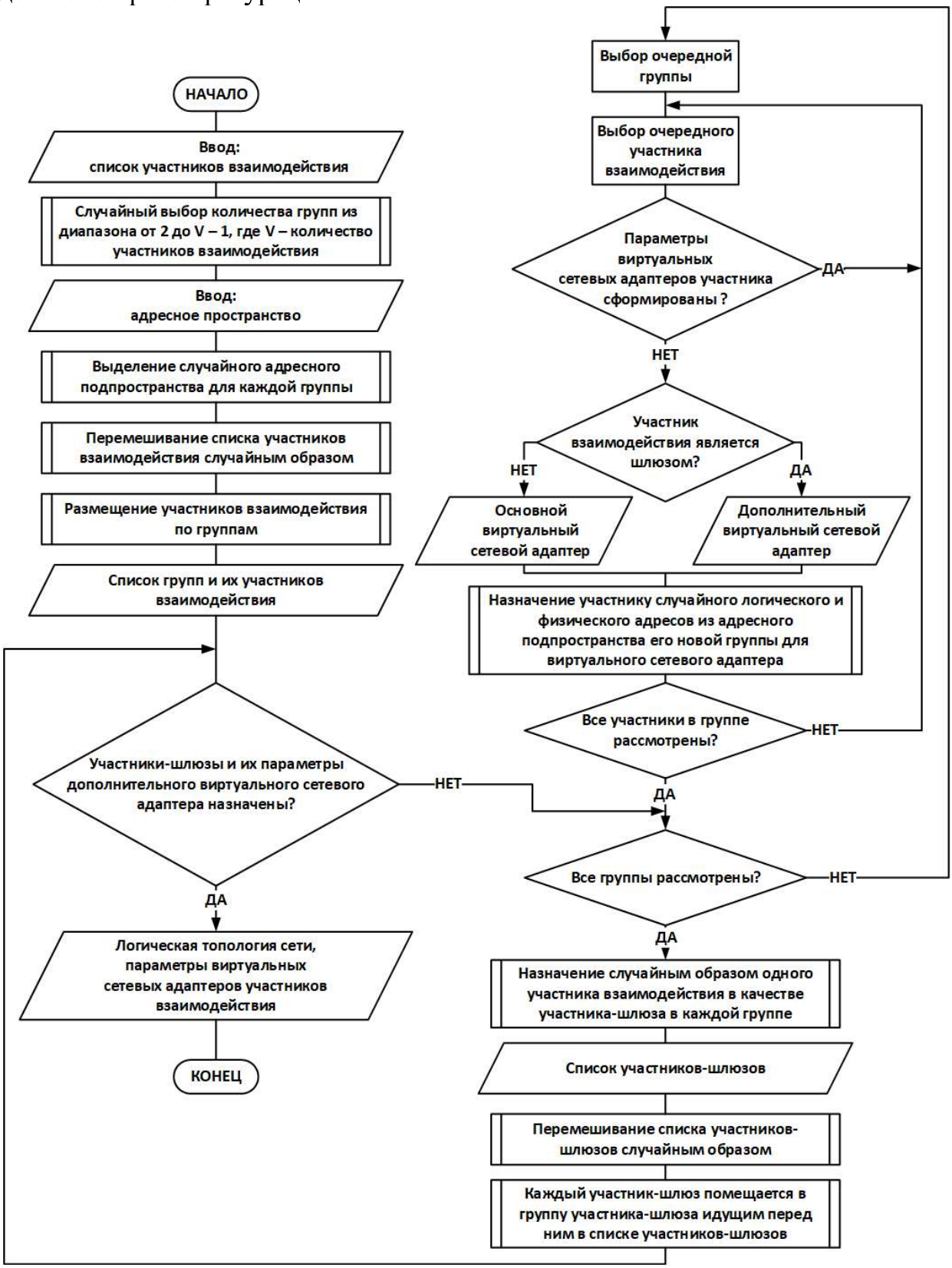

Рисунок 2 – Алгоритм создания логической топологии сети

Для каждой группы выделятся собственное адресное подпространство из адресного пространства всей сети MTD, а каждому участнику взаимодействия – адрес из этого подпространства. Соответствующие сетевые параметры (физический адрес, логический адрес, маска, адрес шлюза, метка группы взаимодействия) задаются для виртуального сетевого адаптера каждого участника взаимодействия. Каждый участник-шлюз имеет два дополнительных виртуальных сетевых адаптера, а обычный участник – только один.

Для того, чтобы участники могли взаимодействовать между собой, участники-шлюзы последовательно-случайно соединяются между собой. Происходит это следующим образом. Все участники-шлюзы помещаются в список, который случайно перемешивается. После чего каждый участник-шлюз вступает в группу участника-шлюза, предыдущего перед ним в списке. Сетевые параметры соответствующей новой группы формируются участником-сервером для второго дополнительного виртуального сетевого адаптера каждого участника-шлюза. Этот новый участник группы становится внешним участником-шлюзом по отношению к новой группе.

Так как алгоритм создания логической топологии сети представляет собой последовательный двойной проход списка участников взаимодействия, его сложность будет составлять $2 \times s$ итераций или $O(n)$.

Для передачи данных участнику-шлюзу необходимо знать куда перенаправить сетевой пакет для достижения пункта назначения: либо внешнему участнику-шлюзу группы, для которой он является внутренним, либо внутреннему участнику-шлюзу группы, для которой он является внешним. Для формирования таблицы маршрутизации также используется массив соединения участников-шлюзов между собой. Массив снова проходится последовательно: сначала в одну сторону, а затем – в обратную. Для каждого участника-шлюза в таблицу маршрутизации добавляется запись о других группах взаимодействия, в которые входят другие участники-шлюзы далее в массиве относительно текущего. В обратную сторону – аналогичным образом. На рисунке 3 показан алгоритм построения маршрутов передачи данных.

Для каждого сетевого устройства формируются управляющие команды по следующему принципу: для интерфейса, к которому подключен участник взаимодействия, задается разрешение на прием-передачу трафика, помеченного метками только тех групп, к которым подключен данный участник взаимодействия и передачу трафика которых ему необходимо осуществлять. Потенциально опасные хосты, для которых принято решение об исключении, в соответствии с правилами исключения могут быть изолированы от взаимодействия соответствующими управляющими командами.

Каждому участнику взаимодействия формируются управляющие команды, которые содержат параметры виртуальных сетевых адаптеров. Предполагается, что взаимодействие между хостами осуществляется при помощи доменных имен, поэтому участник-сервер при создании новой топологии сетевого уровня также формирует список доменных имен и соответствующих

им логических адресов. Для каждого участника взаимодействия также формируются команды, которые содержат этот список.

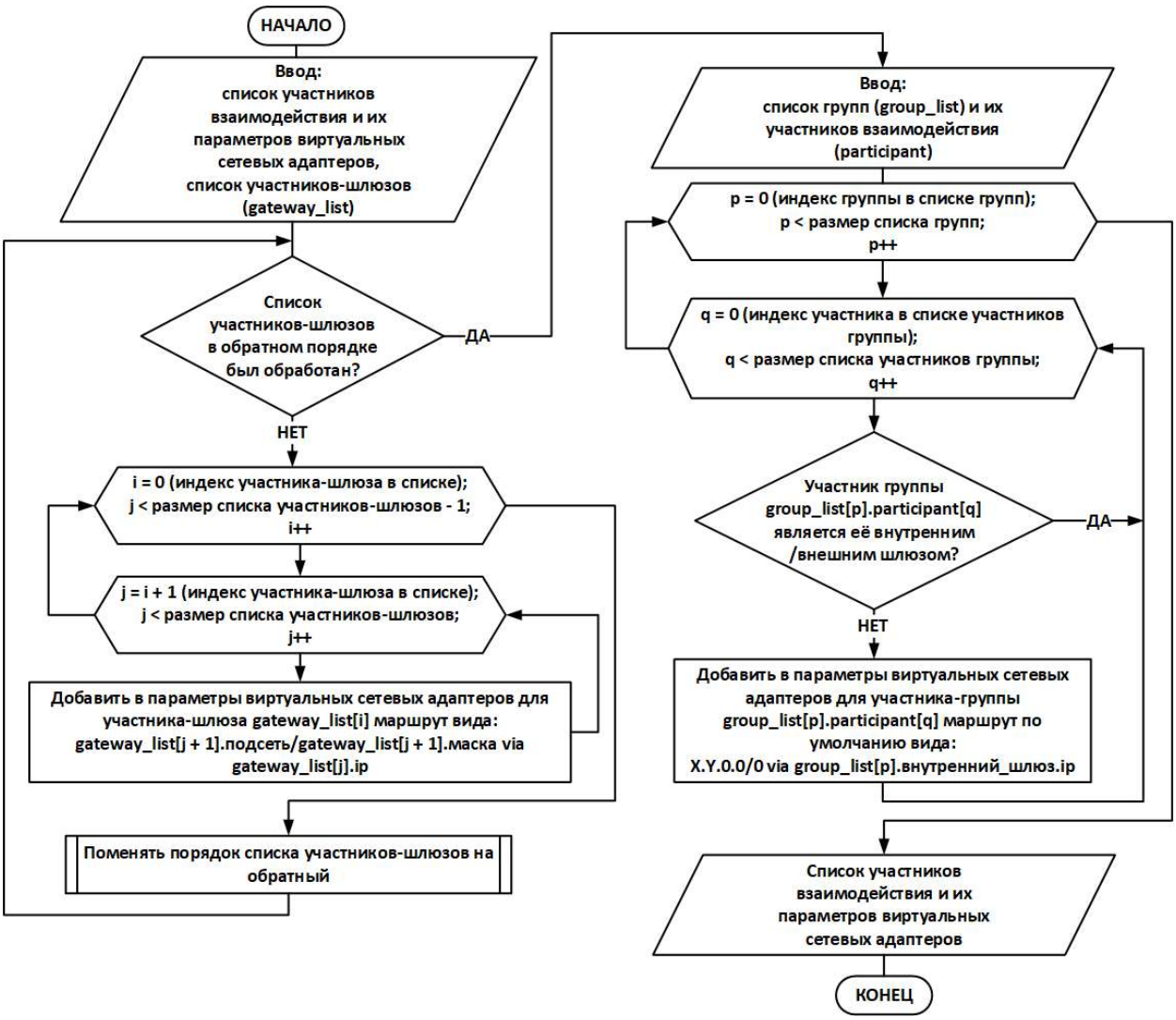

Рисунок 3 – Алгоритм построения маршрутов передачи данных

Сложность алгоритма создания логической топологии сети составит $O(n^2)$, так как алгоритм состоит из:

1. внешний цикл, который проходит по списку шлюзов в прямом и обратном порядке (s итераций или $O(n)$);

2. внутренний цикл для каждого шлюза, который проходит все шлюзы после него в списке ($s/2$ итераций в среднем или $O(n)$);

3. цикл, который проходит по списку групп и их участников взаимодействия (s итераций или $O(n)$).

Поэтому результирующая сложность алгоритма создания логической топологии сети составит $2 \times (O(n) \times O(n)) + O(n)$, что равно $O(n^2)$.

Следует отметить тот факт, что все участники взаимодействия должны быть достижимы участником-сервером. Для того, чтобы организовать сеть MTD, сетевое оборудование должно быть способно управляться программно через сеть, а участник-сервер должен иметь подключение к соответствующим

интерфейсам управления сетевым оборудованием. При этом предполагается, что для управления хостами и сетевым оборудованием выделены отдельные изолированные сети, в которых данные передаются в зашифрованном виде.

Участник-сервер рассылает управляющие команды для сетевого оборудования через их интерфейсы управления. В случае неудачи участник-сервер оповещает об ошибке и прекращает свою работу, так как сеть MTD не может быть сформирована. В случае успеха участник-сервер рассылает параметры для каждого участника взаимодействия. В случае, если участники взаимодействия не сообщили об успешном приеме конфигурации, они исключаются из списка подключенных, а топология сетевого уровня реконфигурируется заново.

Так как алгоритм создания управляющих команд представляет собой последовательный проход физического описания сети, его сложность будет составлять $O(n)$.

Предложенный метод противостоит угрозам следующим образом:

1. Метод и алгоритм динамически изменяют адреса хостов, маршруты передачи данных и логическую топологию через определенные периоды времени или по обнаружению злоумышленника. Собранная информация о сети на периоде между реконфигурациями перестает быть актуальной, так как после реконфигурации хосты располагаются на новых физических и логических адресах.

2. В исследовании сети злоумышленник никак не ограничен до тех пор, пока не будет обнаружен. В случае обнаружения он может быть изолирован при помощи предложенного алгоритма.

3. Предложенный метод и алгоритм никак не препятствуют использованию средств по защите передаваемых данных по сети.

Предложенный метод может быть усилен при помощи:

1. Динамического создания новых ложных хостов, таким образом изменяя количество хостов сети MTD.

2. Динамического реконфигурирования состава и версий сетевых сервисов и служб.

На рисунке 4 приведен стек технологий, который был использован для реализации предложенных метода и алгоритма.

В основе предлагаемого метода лежит программно-управляемая сеть, построенная на технологии VXLAN. VXLAN – это технология виртуализации сети, разработанная для решения проблем масштабируемости и гибкости традиционных сетей Ethernet в крупномасштабных многопользовательских центрах обработки данных и облачных средах. Технология VXLAN позволяет создавать и изменять виртуальные сегменты сети «на лету». Эта ключевая особенность этой технологии, которая позволяет MTD гибко создавать подсети.

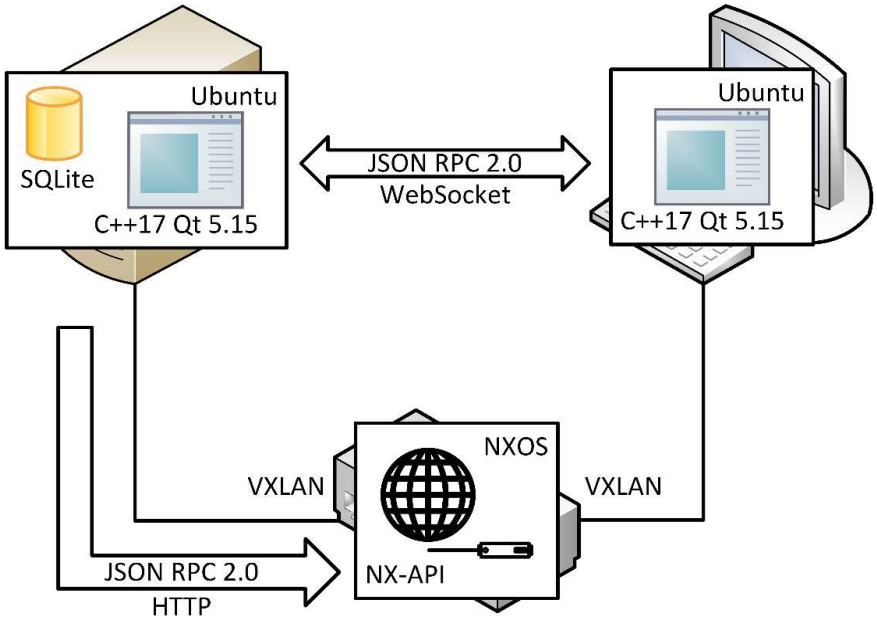

Рисунок 4 – Используемый стек технологий для реализации предложенного алгоритма

Третья глава посвящена анализу эффективности предложенного метода. Несмотря на высокий потенциал MTD, одной из серьезных проблем на пути ее широкого применения является отсутствие единой методологии оценки ее эффективности. В научном сообществе используется ряд характеристик и метрик, по которым можно сравнить существующие решения.

Для метода и алгоритма были получены значения накладных расходов и производительности передачи данных, которые приведены далее в таблице 2. Также была получена оценки окна атаки и вероятности идентификации целевого хоста.

Окно атаки – это непрерывный интервал времени, который злоумышленник может использовать, не прерываясь из-за изменений поверхности атаки. Чем короче окно атаки, тем меньше у злоумышленника времени на действия, что повышает шансы защитников на предотвращение атаки. И наоборот, более длинное окно атаки дает злоумышленнику больше времени для осуществления действий, что потенциально может привести к успешной атаке до того, как произойдет следующая реконфигурация. На основе экспериментальных данных оценки окна атаки можно построить графики зависимости вероятности идентификации целевого хоста от времени сканирования, которые приведены на рисунке 5. Предполагается, что злоумышленник идентифицирует хост как целевой только после завершения сканирования, т.е. когда определит все хосты сети.

Результаты эксперимента подтверждают оценку вероятности идентификации целевого хоста, после каждой реконфигурации эта величина соответствует $1/N$, где N – количество хостов в сети. Злоумышленник вынужден исследовать на каждой итерации сеть заново.

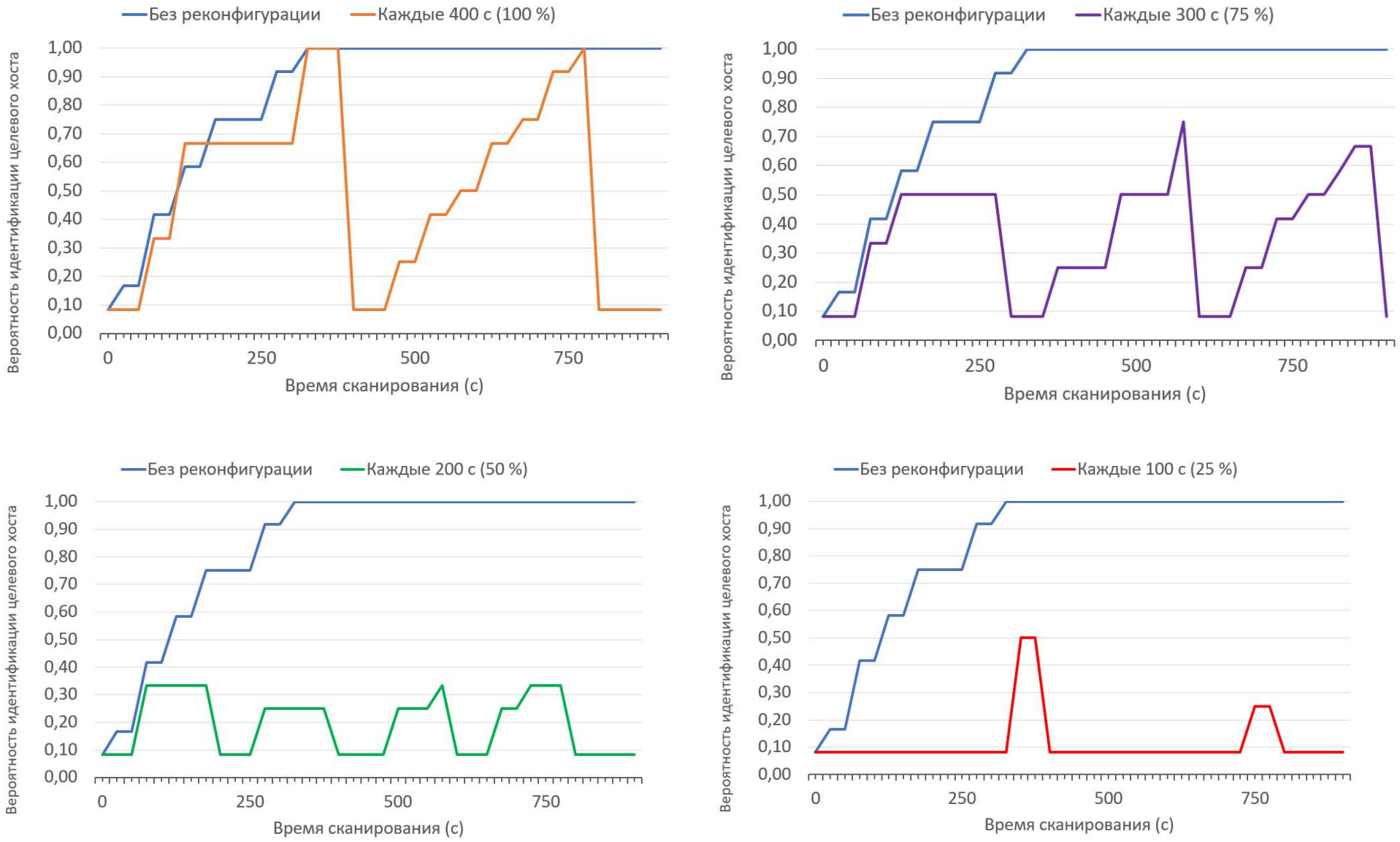

Рисунок 5 – Графики зависимости вероятности идентификации целевого хоста с реконфигурацией сети

В эксперименте злоумышленник сканировал адресное пространство последовательно. Очевидно, зная, как работает предложенный алгоритм, наилучшей стратегией сканирования в данном случае заключается в следующем: зная IP-адрес хоста, в который внедрился злоумышленник, ему достаточно сканировать только ту группу (подсеть), в которой этот хост находится. Предложенный алгоритм работает так, что рано или поздно злоумышленник окажется в одной группе с целевым хостом и ему не нужно сканировать все адресное пространство. Однако, предложенный метод противодействует этому путем исключения потенциально опасных хостов из взаимодействия при обнаружении вредоносной активности (например, сканирование). Кроме того, даже если злоумышленник идентифицирует целевой хост, его время на атаку ограничено периодом реконфигурации. Если злоумышленник не успеет завершить свою атаку, то он будет вынужден искать целевой хост заново. Может пройти значительное время, пока злоумышленник и целевой хост снова окажутся в одной группе. В статичной сети, злоумышленник гарантированно найдет целевой хост.

Для сравнения с существующими решениями были выбраны следующие работы.

1. Dunlop M. Mt6d: A moving target ipv6 defense / M. Dunlop, S. Groat, W. Urbanski [et al.] // 2011-MILCOM 2011 Military Communications Conference. – 2011. – P. 1321-1326.

Эта реализация заключается в периодических изменениях адреса источника и назначения сетевого и транспортного уровней. Изменение адресов может быть произведено в середине текущей сессии без разрыва соединения или необходимости нового рукопожатия. Это может увеличить трудозатраты на атаку для злоумышленника, поскольку адресное пространство IPv6 достаточно велико, а сеансы взаимодействия постоянно меняются. MT6D должна поддерживать несколько IPv6-адресов для каждого узла в любой момент времени.

2. MacFarland D. C. The SDN shuffle: Creating a moving-target defense using host-based software-defined networking / D. C. MacFarland, C. A. Shue // Proceedings of the second ACM workshop on moving target defense. – 2015. – P. 37-41.

Эта реализация основана на подходе перемешивания SDN и использует синтетическую информацию для замены реальной информации об адресации для защиты от исследования злоумышленником. Каждый раз, когда клиент запрашивает DNS-разрешение сервера, SDN-контроллер генерирует синтетические адреса для запрашиваемого сервера и отправляет их на DNS-сервер для ответа клиенту. После чего SDN-контроллер устанавливает правила трансляции сетевых адресов (NAT), которые преобразуют синтетические IP-адреса и MAC-адреса в реальные адреса.

3. Luo Y. B. RPAH: Random port and address hopping for thwarting internal and external adversaries / Y. B. Luo, B. S. Wang, X. F. Wang [et al.] // 2015 IEEE Trustcom/BigDataSE/ISPA. – 2015. – V. 1. – P. 263-270.

Эта реализация основана на подходе случайного перехода по портам и адресам. Клиенты должны использовать различные пары виртуальных адресов и номеров портов для получения услуг в разные временные интервалы. Такая схема адресов и портов позволяет обнаружить злоумышленников, которые будут обращаться к серверам по недействительным адресам и портам.

4. Luo Y. et al. A keyed-hashing based self-synchronization mechanism for port address hopping communication / Y. B. Luo, B. S. Wang, X. F. Wang [et al.] // Frontiers of Information Technology & Electronic Engineering. – 2017. – V. 18, No. 5. – P. 719-728.

В работе приведена реализация MTD с использованием проброса портов, позволяющая обеспечить синхронизацию каждого пакета без использования дополнительных каналов связи. Это достигается путем вычисления кода аутентификации сообщения с ключом-хэшем, который используется не только для проверки целостности данных на стороне получателя, но и в качестве входных данных для алгоритмов кодирования/декодирования пакетов. Также при помощи этого ключа-хэша вычисляются виртуальные адреса и порты, которые будут присвоены сообщению, и сопоставляются с реальными сетевыми данными для восстановления. Такой подход требует использования общего сеансового ключа, известного обеим сторонам. При этом данные в каждом пакете об адресах и портах получателя и отправителя изменяются на каждом переходе при прохождении маршрута.

Эти работы были выбраны по двум причинам. Во-первых, они посвящены защите от исследования злоумышленником именно локальных сетей передачи данных. Во-вторых, опубликованные данные покрывают большую часть перечисленных характеристик и метрик.

Результаты для предложенных метода и алгоритма были получены на тестовом стенде для формирования значений по предложенным критериям. В таблице 1 приведены результаты сравнения по характеристикам, а в таблице 2 – по метрикам.

Одним из главных преимуществ предложенного метода является возможность изоляции злоумышленника в случае его обнаружения. В тоже время большинство методов сконцентрированы на том, чтобы заставить вести себя злоумышленника так, чтобы он выдал себя, например, обращаясь по устаревшим адресам.

Предложенный метод отличается от существующих главным образом разнообразностью набора параметров, которые изменяются в ходе функционирования, а именно изменяющиеся топологией сетевого уровня. Это обеспечивает тот факт, что сеть выглядит для злоумышленника совершенно иным образом на каждой итерации метода, в отличие от других решений, где изменяется лишь часть параметров.

Кроме того, большинство решений MTD сконцентрированы на сокрытии реальных логических и физических адресов хостов сети путем их подмены на фиктивные. В то время как предложенный метод на каждой итерации изменяет реальные адреса хостов. Даже в том случае, если злоумышленник

выяснит настоящий адрес, он устареет в отличие от других решений MTD, основанных на подмене адресов.

Также предложенный метод, в отличие от других, имеет механизмы адаптации. В случае обнаружения злоумышленника топология сетевого уровня может быть сконфигурирована так, что злоумышленник может быть исключен или изолирован. В то время как остальные решения полагаются на то, что злоумышленник выдаст себя, если воспользуется неактуальной информацией, а защитники примут соответствующие меры по противодействию злоумышленнику.

Таким образом, предложенный метод лучше остальных решений MTD по следующим характеристикам: подход к изменению параметров, адаптивность и разнообразность изменения поверхности атаки. Хотя предложенный метод обладает большей разнообразностью изменения поверхности атаки, но при этом именно это является причиной высоких задержек, вносимых при смене одной топологии сетевого уровня на другую. Текущее на момент написания диссертационного исследования состояние возможностей сетевого оборудования по смене топологии сетевого уровня не позволяет сократить эти задержки. Предложенный метод манипулирует более широким набором реальных параметров, включая логическую топологию сети, и управляет сетевым оборудованием, поэтому задержки, вносимые при смене одной конфигурации на другую длительны относительно других решений, а соответственно и снижение производительности передачи данных более существенно.

Существующие решения манипулируют более ограниченным набором параметров, а чаще всего просто подменяют эти параметры [96, 116, 117]. Поэтому в других решениях отсутствуют длительные задержки в сети. Но при этом предложенный метод обеспечивает тот факт, что сеть для злоумышленника выглядит совершенно новым образом на каждой итерации метода. Предложенный метод после перехода на новую топологию сетевого уровня вынуждает злоумышленника начинать исследование сети заново, так как хосты будут иметь новые физические и логические адреса, а сеть – новую логическую топологию и маршруты. Тогда как в других решениях изменяется лишь часть параметров сети.

Степень снижения производительности не делает предложенный метод неприменимым для защиты от исследования злоумышленником. Однако, для ИС чувствительным к задержкам он может быть неприменим. При этом, это не является недостатком самого предложенного метода. Такие задержки связаны именно с несовершенством сетевого оборудования, так как требуется время сетевому оборудованию для смены конфигурации на другую. Таким образом, с развитием сетевого оборудования по части сокращения длительности смены одной конфигурации на другую, негативное влияние предложенного метода на производительность сети также будет сокращаться.

Таблица 1 – Сравнение с существующими решениями по характеристикам

Характеристика	Предлагаемый метод	Dunlop M. (et al.)	MacFarland D. C. (et.al)	Luo Y. (et al.) 2015	Luo Y. (et al.) 2017
Подход к созданию пространства конфигураций	«На лету».	«На лету».	«На лету».	«На лету».	«На лету».
Схема управления	Централизованная.	Централизованная.	Централизованная.	Централизованная.	Децентрализованная.
Подход к изменению параметров	Изменение реальных значений параметров.	Изменение реальных значений параметров.	Подмена реальных значений параметров фиктивными.	Подмена реальных значений параметров фиктивными.	Подмена реальных значений параметров фиктивными.
Адаптивность	Есть.	Нет.	Нет.	Нет.	Нет.
Разнообразность изменения поверхности атаки	Физические адреса; Логические адреса; Маршруты передачи данных; Логическая топология сети.	Физические адреса; Логические адреса; Ключи шифрования.	Физические адреса; Логические адреса.	Физические адреса; Логические адреса; Порты.	Физические адреса; Логические адреса; Порты.
Способ генерации параметров	Случайности.	Случайности.	Хэш-функция.	Хэш-функция.	Хэш-функция.
Своевременность	Фиксированный период; Событие.	Динамический период.	Событие.	Фиксированный период.	Событие.

Таблица 2 – Сравнение с существующими решениями по метрикам

Метрика	Предлагаемый метод	Dunlop M. (et al.)	MacFarland D. C. (et.al)	Luo Y. (et al.) 2015	Luo Y. (et al.) 2017
Накладные расходы адресного пространства	До 65534 адресов сети.	Нет данных.	Нет данных.	Нет данных.	Нет данных.
Накладные расходы на передачу	Генерирует в среднем 3600 байт на один хост сети за одну реконфигурацию.	62 байта на каждый сетевой пакет.	Отсутствуют.	Отсутствуют.	Отсутствуют
Накладные расходы на маршрутизацию	Длина маршрута увеличивается от 0 до $N-1$ переходов, где N – кол-во хостов.	2 дополнительных перехода.	1 дополнительный переход.	Отсутствуют.	Отсутствуют.
Производительность передачи данных	Снижает в среднем до 27 %	Снижает до 5 %	Не влияет	Снижает до 10 %	Снижает до 1 %.
Задержки при переходе от одной конфигурации к другой	от 30 до 46 с	12 мс	20 мс	5 с	Отсутствуют
Нагрузка на сетевое оборудование	до 40 % ЦП, до 20 % ОЗУ	Нет данных	Нет данных	Нет данных	Нет данных

Поэтому проблему с производительностью можно решить способами, которые расположены по степени влияния на производительность от наибольшего к наименьшему:

1. сокращение времени смены конфигураций сетевого оборудования;
2. сокращение времени смены параметров виртуальных сетевых адаптеров на хостах сети;
3. переориентация приложение и протоколов на использование доменных имен и внедрение механизмов восстановления соединения в случае, если в процессе сеанса связи изменились адреса;
4. адаптация приложений и протоколов под постоянно изменяющиеся адреса хостов и под текущие характеристики производительности.

Текущее влияние на производительность передачи данных и стабильность всей сети приемлемо для ИС нечувствительным к задержкам, при этом положительный эффект, оказываемый на защиту локальной сети передачи данных от исследования злоумышленником, достаточно высок относительно аналогичных решений.

Таким образом предложенный метод является перспективным. Предложенный метод был апробирован и внедрен в АО «НПП «Радиосвязь» и СибГУ им. М. Ф. Решетнева

В заключении представлены основные результаты и выводы, полученные в ходе проведения диссертационного исследования.

В приложениях приведены документы, подтверждающие внедрение, свидетельства о регистрации программ для ЭВМ.

Основные выводы и результаты

1. Проанализированы современные стратегии ИБ, а именно концепция активного и пассивного подхода к ЗИ. Пассивный подход к ЗИ опирается на заранее определенные эшелоны защиты, которые остаются неизменными, что делает ИС уязвимой для злоумышленника, который может использовать известные уязвимости чтобы обойти эти эшелоны. В свою очередь активный подход к ЗИ предполагает постоянную адаптацию к изменяющимся угрозам.
2. Проанализированы СЗИ, применяемые в рамках активного подхода, а именно технологии ИО и MTD. Данные технологии часто применяются в совокупности друг с другом и предназначены для введения злоумышленника в заблуждение. Несмотря на то, что существующие реализации данных технологий имеют существенные ограничения, они имеют перспективу для применения: введение в заблуждение на стадии сетевой разведки подрывает эффективность всей атаки злоумышленника. В случае его проникновения внутрь сети, существующие СЗИ не всегда способны противодействовать разведке сети, таким образом применение таких технологий обосновано.
3. Разработан модифицированный итерационный метод защиты локальной сети передачи данных от стороннего исследования, отличающийся от существующих подходом к созданию подвижных целей, основанном на перегруппировке хостов в сочетании с рандомизацией адресов и маршрутов. Данный метод предполагает такое реконфигурирование топологии сетевого уровня, при котором её параметры (поверхность атаки) изменяются по

наступлению событий или истечению временно́го периода. Предложенный итерационный метод позволяет изменить поверхность атаки до состояния, при котором множество хостов, идентифицированных злоумышленником, соответствует пустому множеству при каждой его итерации. В результате при каждой реконфигурации злоумышленник вынужден исследовать сеть заново.

5. Разработана модифицированная математическая модель оценки защищённости сети, формируемой на основе предложенного метода, при помощи которой установлено, что вероятность идентификации целевого хоста на каждой итерации метода составляет $1/N$, где N – количество хостов сети, в отличие от статичной сети, где вероятность в процессе её исследования стремится к 1.

6. Разработан новый алгоритм формирования топологии сетевого уровня и реализующее его программное средство, предназначенные для защиты от исследования злоумышленником локальной сети передачи данных. Благодаря тому, что метод является итерационным, он позволяет свести множество хостов, идентифицированных злоумышленником, к пустому, а алгоритм формирования топологии сетевого уровня при каждом его повторном использовании создает одну новую работоспособную топологию из всех возможных топологий и сводит вероятность идентификации целевого хоста к $1/N$, где N – это количество хостов сети MTD. Алгоритм формирования топологии сетевого уровня периодически заново используется для генерации новой топологии сетевого уровня, тем самым обеспечивая её постоянную реконфигурацию.

4. Предложенные метод и алгоритм были реализованы на основе следующих технологий: протокол канального и сетевого уровня модели OSI – VXLAN, протокол взаимодействия с хостами сети – протокол собственной разработки на основе JSON RPC 2.0 через WebSocket, протокол взаимодействия с сетевым оборудованием – протокол спецификации NX-API на основе JSON RPC 2.0 через HTTP, ОС хостов сети – Ubuntu 22.04, ОС сетевого оборудования – NX-OS, СУБД – SQLite, программный код – C++17 и Qt 5.15.

5. Был проведен анализ эффективности предложенного метода защиты локальной сети передачи данных от исследования на основе реконфигурации топологии сетевого уровня. Анализ эффективности предложенного метода был проведен на основе его сравнения с существующими аналогичными решениями по характеристикам и метрикам, которые используются в научном сообществе. Характеристики включают в себя: подход к созданию пространства конфигураций, схема управления, подход к изменению параметров, адаптивность, разнообразность изменения поверхности атаки, способ генерации параметров и своевременность. Метрики включают в себя: нагрузка на сетевое оборудование, накладные расходы адресного пространства, накладные расходы на передачу, накладные расходы на маршрутизацию, пропускная способность, потери пакетов и задержки.

6. В результате оценки эффективности предложенного метода по характеристикам получено следующее. Предложенный метод выгодно отличается

от существующих решений MTD по нескольким характеристикам. Во-первых, это разнообразность изменения поверхности атаки, которая заключается в более широком относительно других решений наборе изменяемых параметров сети, который включает в себя: физический и логический адрес, маршруты передачи данных, логическая топология сети. Во-вторых, числовые значения этих параметров генерируются случайным образом при каждой реконфигурации, тем самым изменяется поверхность атаки. При этом изменяются реальные значения параметров, в отличие от других решений, где в большинстве своем применяется подмена реальных параметров фиктивными значениями. В-третьих, это адаптивность, которая заключается в наличии механизмов по реконфигурированию сети в результате обнаружения злоумышленника и, при необходимости, в реконфигурировании таким образом, чтобы злоумышленник был изолирован.

7. Для оценки эффективности предложенного метода по метрикам был взят предложенный алгоритм и реализующее его программное средство. Были получены следующие результаты. Предложенный алгоритм незначительно нагружает сетевое оборудование. Предложенный алгоритм поддерживает до 65534 адресов в сети MTD. Предложенный алгоритм генерирует в среднем 3600 байт на одного участника взаимодействия и 8416 байт на одно сетевое устройство на каждой реконфигурации. Реализация предложенного алгоритма создает временные периоды, когда передача данных невозможна, длительностью от 30 до 46 секунд. Такая длительность этих периодов вызвана именно изменениями конфигураций сетевого оборудования. Экспериментально было установлено то, что изменение параметров виртуальных сетевых адаптеров и маршрутов на хостах сети происходит в течение времени от 2 до 5 секунд. Когда топология сетевого уровня уже развернута, предложенный алгоритм никак не влияет на производительность сети.

8. Была проведена оценка окна атаки для предложенного алгоритма и реализующего его программного средства. Предложенный алгоритм сокращает окно атаки для злоумышленника, изменяя поверхность атаки, на величину, которая зависит от выбранного периода. После каждой реконфигурации, оценка вероятности идентификации целевого хоста составляет $1/N$, где N – это количество хостов сети. Данная оценка получена эмпирически.

9. Для того, чтобы улучшить производительность сети при использовании предложенного алгоритма, необходимо сокращать длительность смены одной топологии сетевого уровня на другую. Снижение производительности сети связано именно с недостатками существующих сетевых устройств по части смены одной конфигурации на другую, так как, на момент написания работы, эта операция требует значительного времени. Текущее влияние на производительность передачи данных и стабильность сети приемлемо для ИС нечувствительным к задержкам. Таким образом можно сделать вывод о том, что предложенный метод является перспективным.

10. Предложенный алгоритм и реализующее его программное средство были внедрены в имитатор станции связи АО «НПП «Радиосвязь» для анали-

за потенциальной применимости технологии MTD для защиты от исследования злоумышленником схем организации связи, топологии и состава станции. Предложенные метод и алгоритм показали свою потенциальную применимость для некоторых схем организации связи, нечувствительных к задержкам. Также предложенный метод был внедрен в образовательный процесс СибГУ им. М. Ф. Решетнева для практического ознакомления студентов со способами и средствами исследования локальных сетей передачи данных, а также современными подходами по противодействию исследованию злоумышленником сети.

11. В результате анализа внедрения было получено, что для эффективного применения предложенного метода необходимо найти баланс между частотой реконфигураций и приемлемым уровнем производительности передачи данных. Частота реконфигурации индивидуальна для каждой сети, и она может быть найдена при помощи предложенной математической модели и проведенных экспериментов.

Диссертация представляет собой законченную самостоятельную научно-квалификационную работу, в которой решена научная задача защиты от исследования злоумышленником локальной сети передачи данных при помощи динамических реконфигураций топологии сетевого уровня.

Дальнейшие перспективы работы в рамках рассмотренной тематики заключаются в расширении набора изменяемых параметров и в сокращении длительности периодов, возникающих при смене одной топологии сетевого уровня на другую, когда передача данных невозможна. Таким образом, все задачи, поставленные в рамках диссертационного исследования, были выполнены.

Список основных публикаций по теме диссертации

Публикации в изданиях, рекомендованных ВАК РФ:

1. Паротькин Н. Ю., Панфилов И. А., Золотарев В. В., Кушко Е. А., Панфилова Т.А. Разработка и экспериментальное исследование протокола динамического адресного пространства на основе мультикаст-групп // Сибирский журнал науки и технологий. – 2017. – Т. 18, №4. – С. 779-787.

2. Кушко Е. А. Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. 2020. № 4. С. 39-52.

3. Кушко Е. А., Грачев Д. А., Паротькин Н. Ю., Золотарев В. В. О вопросах безопасности киберфизических систем // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2022. – Т. 25, № 4. – С. 101-109.

4. Кушко Е. А., Паротькин Н. Ю., Золотарев В. В. Организация защищенного обмена внутри программно-управляемой локальной сети // Вестник СибГУТИ. – 2023. – Т. 17, № 4. – С. 62-73.

5. Кушко Е. А., Трофимычев И. И. Метод защиты от исследования локальной вычислительной сети на основе реконфигурации топологии сетевого уровня // Прикаспийский журнал: управление и высокие технологии. – 2024. – № 3(67). – С. 63-72.

Публикации в изданиях, индексируемых в международных базах:

1. E. A. Kushko, N. Yu. Parotkin. The research of technologies for secure data communication in dynamic networks // IEEE Xplore Digital Library, Dynamics of Systems, Mechanisms and Machines (Dynamics). 2017.

2. E. A. Kushko, N. Yu. Parotkin. Software implementation details of the secure data communication protocols stack based on the dynamic network topology // Journal of Physics: Conference Series 1399, IOP Publishing, 2019.

3. E. A. Kushko, N. Yu. Parotkin. Efficiency Evaluation of Secure Data Communication Protocols Stack Based on Dynamic Network Topology // 2019 International Russian Automation Conference, Rusautocon, IEEE, 2019.

4. E. A. Kushko, N. Yu. Parotkin. Method of hiding the architecture and configuration of the sensor network based on the dynamic topology // IOP Conference Series: Materials Science and Engineering. 2020. 862. 052024.

5. E. A. Kushko, N. Yu. Parotkin. Concealment of sensor network node interaction // IOP Conference Series: Materials Science and Engineering. III International Scientific Conference. Krasnoyarsk, 2021. С. 12058.

В других изданиях, сборниках трудов и тезисов конференций:

1. Паротькин Н. Ю., Кушко Е. А., Арифанова Н. В. Реализация элементов динамического адресного пространства // Актуальные проблемы авиации и космонавтики. 2016. Т. 1. № 12. С. 760-762.

2. Кушко Е. А. О решении задачи обеспечения защищенного обмена данными в локальной сети // Актуальные проблемы авиации и космонавтики. 2018. Т. 2. № 4 (14). С. 229-231.

3. Кушко Е. А. Метод обеспечения защиты передаваемых данных на основе плавающей топологии сети // Решетневские чтения. 2018. Т. 2. С. 337-338.

4. E. A. Kushko. Ways to improve the performance of secure data communication protocols stack based on the dynamic network topology // Актуальные проблемы авиации и космонавтики. 2019. Т. 2. С. 237-238.

5. Кушко Е. А. Детали технического решения по обеспечению сокрытия архитектуры и конфигурации сенсорной сети // Решетневские чтения. 2020. Т. 2. С. 526-527.

6. Кушко Е. А. Способ реализации сокрытия архитектуры и конфигурации сенсорной сети // Актуальные проблемы авиации и космонавтики. 2020. Т. 2. С. 233-235.

7. Кушко Е. А. О вопросах безопасности передачи данных в сенсорной сети // Актуальные проблемы авиации и космонавтики. 2021. Т. 2. С. 384-386.

8. Кушко Е. А. Обеспечение защищённого обмена данными методами нестационарной топологии взаимодействия узлов // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума "Информационная безопасность - 2021"). 2021. С. 90-95.

9. E. A. Kushko, N. Yu. Parotkin. Formalization of secure data communication implementation method based on dynamic network topology // Наука, технологии, общество - НТО-II-2022. 2022. – P. 78-87.

Свидетельства о регистрации программы для ЭВМ:

1. 2022669450, 01.11.2022, «Программный модуль реализации защищенного обмена данными на основе динамической топологии сети»