МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет науки и технологий
имени академика М. Ф. Решетнева»

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

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель –
кандидат технических наук, доцент
Золотарев В. В.

Красноярск – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 техно-

логий (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 либо 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. Использовались 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-практической конференции, 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. Диссертационная работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2023-2025 гг. (проект № FEWM-2023-0015).

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, списка сокращений, словаря терминов, библиографического списка из 136 цитируемых источников, 5 приложений, а также 34 рисунков и 10 таблиц.

1. Проблема защиты локальных сетей передачи данных от исследования злоумышленником

1.1 Современные стратегии информационной безопасности

В условиях все более широкого проникновения информационных технологий (ИТ) во все отрасли экономики стратегии ИБ развиваются, чтобы противостоять растущей сложности и изощренности угроз. Современные стратегии ИБ включают в себя различные подходы, в том числе традиционную защиту периметров, так и новые подходы, которые направлены на раннее обнаружение и противодействия угрозам.

1.1.1 Модель цепочки атаки

Основополагающей в области ИБ является модель Cyber Kill Chain [1], представленная компанией Lockheed Martin в 2011 году. Основная цель ее заключается в том, чтобы предложить защитникам структурированную методологию для понимания того, как происходит процесс атаки. Это позволит защитникам эффективнее обнаруживать, реагировать и устранять угрозы. Предпроверяя атаку на составляющие ее стадии, Cyber Kill Chain позволяет получить более полное представление о тактике злоумышленника и понять, какие именно стратегии он использует. Это делает модель Cyber Kill Chain важным инструментом для защиты от современных APT-атак.

Первой стадией Cyber Kill Chain является разведка (Reconnaissance). Разведка заключается в процессе, в котором злоумышленник проводит предварительное исследование атакуемой ИС для определения возможных целей и сбора необходимой информации. Эта стадия является очень важной для злоумышленника, так как она помогает ему понять окружение атакуемой ИС, включая ее сетевую структуру, уровень безопасности и возможные уязвимости. В зависимости от того, какая стратегия разведки применяется, разведка может быть, как пассивной, то есть наблюдение без прямого взаимодействия с ИС, так и активной, когда злоумышленник взаимодействует с ИС, чтобы выявить её уязвимости. Проведение успешной разведки определяет точность

и эффективность последующих действий, что позволяет считать стадию разведки критической точкой для осуществления защитниками раннего обнаружения и противодействия.

Вторая стадия Cyber Kill Chain – вооружение (Weaponization). Злоумышленник на стадии вооружения разрабатывает вредоносное программное обеспечение (ВПО), которое предназначено для эксплуатации обнаруженных уязвимостей. Далее злоумышленнику необходимо соединить ВПО с механизмом доставки, например, с фишинговым письмом или взломанным вебсайтом. Полезная нагрузка доставки может включать в себя различные виды ВПО, такие как вирусы, черви и программы-вымогатели, которые используются для проникновения внутрь атакуемой ИС. Вооружение – это подготовительный этап, в ходе которого злоумышленник готовит свои инструменты к вторжению. Эта стадия является ключевой, когда защитники потенциально могут выявить и предотвратить атаку, анализируя данные о потенциальных угрозах и отслеживая индикаторы компрометации (Indicator of Compromise, IoC).

Третьей стадией Cyber Kill Chain является доставка (Delivery). На стадии доставки происходит передача полезной нагрузки в целевую среду. При этом могут использоваться различные векторы: вложения в электронную почту, вредоносные ссылки, физические носители и так далее. Она представляет собой первое (в случае, если разведка была пассивной) непосредственное взаимодействие злоумышленника с атакуемой ИС. Эффективные меры ИБ, такие как фильтрация электронной почты, фильтрация веб-страниц и защита конечных точек, необходимы на данной стадии для перехвата полезной нагрузки до того момента, как она достигнет своей цели.

Четвертая стадия Cyber Kill Chain – эксплуатация (Explotation). После успешного завершения доставки следует стадия эксплуатации, во время которой злоумышленник выполняет свою полезную нагрузку на целевой системе. Использование уязвимостей программного обеспечения (ПО), оборудования или людей для получения несанкционированного доступа является распро-

страненной практикой на стадии эксплуатации. Данная стадия характеризуется активацией ВПО, которое может использовать уязвимости в операционной системе (ОС), ПО или поведении пользователя. В момент начала эксплуатации атака переходит от подготовки к выполнению, что является также критическим моментом для защитников, чтобы обнаружить вредоносную активность и предотвратить осуществление атаки.

Пятой стадией Cyber Kill Chain является установка (Installation). На стадии установки злоумышленник обеспечивает себе постоянное присутствие в атакуемой ИС с помощью установки ВПО или бэкдора. Это дает злоумышленнику возможность сохранить доступ, даже в том случае, если изначальная точка проникновения была обнаружена и устранена. На данной стадии злоумышленник может установить дополнительные инструменты для дальнейшей эксплуатации уязвимостей или повышения своих привилегий. Установка является ключевой стадией злоумышленника для обеспечения долговременного контроля над ИС. Для защитников необходимо своевременное обнаружение и удаление установленного ВПО для предотвращения дальнейшего ущерба.

Шестая стадия Cyber Kill Chain – управление и контроль (Command and Control, C2). Во время данной стадии злоумышленник устанавливает канал связи между скомпрометированной ИС и своим удаленным сервером. Это даёт злоумышленнику возможность отдавать команды, осуществлять эксфильтрацию данных и увеличивать свою полезную нагрузку. Канал управления и контроля является ключевым компонентом для проведения успешной атаки, поскольку он позволяет злоумышленнику сохранить контроль над скомпрометированной ИС. Защитникам необходимо обнаружить и прерывать канала управления и контроля, так как в результате этого злоумышленник потеряет контроль над ИС и, как следствие, уменьшатся масштабы взлома.

Седьмой и последней стадией Cyber Kill Chain является достижение цели (Actions on Objectives). На заключительной стадии злоумышленник реализует свои основные цели, которые могут включать в себя утечку данных,

нарушение функционирования ИС, саботаж или дальнейшее перемещение по сети. Эта стадия является кульминацией атаки, которая должна обеспечить реализацию целей злоумышленника. Необходимо отметить, что действия по достижению целей могут различаться в зависимости от намерений злоумышленника. Они могут включать в себя как кражу интеллектуальной собственности, так и распространение ВПО. На данной стадии можно наблюдать наиболее явные последствия атаки. Своевременное реагирование и эффективное устранение последствий инцидента ИБ имеет решающее значение для смягчения ущерба и восстановления нормальной работы.

За счет системного подхода к анализу угроз и защите от них модель Cyber Kill Chain получила большую известность. Разбивая процесс атаки на отдельные стадии, эта модель позволяет защитникам разрабатывать и применять конкретные меры для предотвращения атак, а также более эффективно реагировать на них. Концентрация модели на раннем обнаружении и вмешательстве защитников особенно ценен в борьбе с APT-атаками, где способность защитников прервать атаку до того, как она достигнет своей финальной стадии, может значительно снизить потенциальный ущерб. Противодействие злоумышленнику именно на стадии разведки снижает потенциальный ущерб до минимального уровня.

1.1.2 Стратегия защиты в глубину

Стратегия защиты в глубину (Defense-in-Depth, DiD) [2] – это стратегия ИБ, которая предусматривает использование нескольких эшелонов безопасности для защиты ИС. Если Cyber Kill Chain представляет собой структурированную основу для понимания стадий атаки, то DiD предлагает модель защиты от таких атак. Эта стратегия, изначально заимствованная из военной науки, где несколько эшелонов обороны используются для задержки и ослабления наступления противника, была адаптирована к ИБ для борьбы со сложными и эволюционирующими угрозами ИБ. Главный принцип DiD заключается в том, что ни одна мера ИБ не является сама по себе надежной, а вместо этого используется большой комплекс мер для обеспечения избыточ-

ности и устойчивости защиты, гарантирующих, что, если один эшелон будет преодолен, другие продолжат защищать ИС.

Основные принципы DiD:

1. Многоуровневые СЗИ. В основе DiD лежит использование многоуровневых СЗИ, которые работают вместе для защиты ИС. Эти уровни могут включать физическую безопасность, сетевую безопасность, безопасность конечных точек, безопасность приложений и безопасность данных. Каждый уровень предназначен для устранения конкретных уязвимостей и потенциальных векторов атак. Например, межсетевые экраны (МЭ) и средства обнаружения вторжений (СОВ) защищают периметр сети, а шифрование и контроль доступа обеспечивают защиту данных внутри ИС.

2. Избыточность и устойчивость. В DiD особое внимание уделяется избыточности, что означает наличие множества дублирующих друг друга мер ИБ, гарантирующих, что в случае отказа одной меры другие смогут защитить ИС. Такая избыточность повышает устойчивость защиты к атакам, не позволяя одной точке отказа поставить под угрозу всю ИС.

3. Разнообразие СЗИ. Еще одним ключевым аспектом DiD является разнообразие СЗИ, которое предполагает использование различных средств и методов обеспечения ИБ для защиты ИС. Такое разнообразие гарантирует то, что, если злоумышленнику удастся обойти один тип защиты, он может не преодолеть другой. Например, в средствах антивирусной защиты (САВЗ) обнаружение ВПО может быть, как на основе сигнатур, так и на основе анализа поведения, что обеспечивает более широкий спектр защиты, поскольку различные методы направлены на борьбу с одними и теми же угрозами.

4. Мониторинг и обнаружение. Непрерывный мониторинг и обнаружение являются неотъемлемыми компонентами DiD. Постоянно анализируя сетевой трафик, поведение пользователей и системные журналы, защитники могут обнаружить аномалии, которые могут свидетельствовать о нарушении ИБ.

Несмотря на эффективность этой стратегии в обеспечении избыточности и устойчивости, ей присущ ряд недостатков, которые становятся все более очевидными перед лицом современных сложных угроз. DiD традиционно основывается на защите «периметров» и на таких средствах ИБ, как МЭ, СОВ и САВЗ, которые предназначены для защиты от известных угроз на «периметре». Однако такой подход является существенным ограничением перед лицом современных APT-атак, уязвимостей «нулевого дня» и других сложных атак, способных обойти традиционные СЗИ [3].

Попав внутрь сети, злоумышленник может перемещаться в ней. DiD по своей сути не предотвращает горизонтальное перемещение, что облегчает злоумышленнику повышение привилегий и доступ к данным. DiD часто работает на основе предположения, что объектам и субъектам, находящимся внутри сети, можно доверять [4]. Такое доверие является значительной уязвимостью, поскольку угрозы от лица внутреннего злоумышленника могут нанести более значительный ущерб, а его обнаружение наступает только после реализации атаки.

Эти недостатки подчеркивают необходимость перехода к другим стратегиям ИБ, которые предлагают более динамичный и адаптивный подход. В отличие от DiD, архитектура нулевого доверия устраняет эти недостатки путем фундаментального переосмысления того, как реализуется ИБ. Архитектура нулевого доверия работает по принципу «никогда не доверяй, всегда проверяй», гарантируя, что ни один объект или субъект, как внутри, так и вне ИС, не является изначально доверенным.

1.1.3 Архитектура нулевого доверия

Архитектура нулевого доверия (Zero Trust Architecture, ZTA) [5] предлагает такую стратегию ИБ, которая в корне меняет подход защитников к обеспечению ИБ. В отличие от традиционных стратегий ИБ, которые исходят из того, что всему, что находится внутри периметра защиты, можно доверять, ZTA основывается на принципе, что ни одному объекту, будь то внутри или

вне ИС, нельзя доверять. ZTA стала главной стратегией ИБ в ответ на ограничения защитных систем, основанных на защите «периметра».

Основные принципы нулевого доверия:

1. Никогда не доверяй, всегда проверяй. Это основополагающий принцип ZTA заключается в устранении неявного доверия в ИС. Каждый пользователь, устройство и приложение должны быть проверены перед предоставлением доступа к ресурсам ИС. Этот процесс проверки является непрерывным, обеспечивая аутентификацию, авторизацию и шифрование каждого соединения, а не полагаясь на одноразовую проверку на периметре сети.

2. Доступ с наименьшими привилегиями. ZTA выступает за предоставление пользователям минимального уровня доступа, необходимого для выполнения их задач, по принципу наименьших привилегий. Ограничивая доступ только необходимым, защитники могут минимизировать потенциальный ущерб, наносимый внутренним злоумышленником. Контроль доступа обеспечивается с помощью ролевого управления доступом, многофакторной аутентификацией и контекстно-зависимых политик, учитывающих такие факторы, как местоположение пользователя, уровень безопасности устройства и его поведение.

3. Микросегментация. Микросегментация – еще один важный компонент ZTA. Она подразумевает разделение сети на небольшие изолированные сегменты и защиту каждого сегмента по отдельности. Это гарантирует, что даже если один сегмент будет взломан, злоумышленник не сможет легко перемещаться по сети. Каждый сегмент применяет свои собственные политики безопасности, требуя аутентификацию и авторизацию для доступа, тем самым сдерживая злоумышленника.

4. Непрерывный мониторинг и анализ. ZTA в значительной степени зависит от непрерывного мониторинга и анализа в режиме реального времени. Постоянно анализируя поведение пользователей, состояние устройств и сетевой трафик, защитники могут обнаруживать аномалии, которые могут свидетельствовать об инциденте ИБ, и реагировать на него. Передовые технологии

обнаружения угроз, включая искусственный интеллект (ИИ) и машинное обучение (МО), часто интегрируются в ZTA, чтобы обеспечить прогнозирование и автоматизацию реагирования на угрозы ИБ.

5. Предположение нарушения. ZTA основана на предположении, что нарушение либо уже произошло, либо может произойти в любой момент. Такой подход побуждает защитников сосредоточиться на минимизации последствий атаки путем сегментации, строгого контроля доступа и быстрого реагирования на инциденты. Предполагая, что злоумышленник может присутствовать в сети, ZTA сокращает время, которое есть у злоумышленника для использования уязвимостей.

Внедрение принципов ZTA стало возможным благодаря развитию автоматизации процессов обеспечения ИБ [6]. Автоматизация позволяет осуществлять непрерывный мониторинг, аутентификацию в режиме реального времени и динамическое применение политик, что является центральным элементом ZTA. Такие задачи, как идентификация и аутентификация, контроль доступа, обнаружение аномалий, могут быть автоматизированы, что обеспечивает последовательное применение политик безопасности без задержек, присущих ручным процессам. Автоматизация также поддерживает масштабируемость ZTA, управляя огромными объемами данных и событий ИБ, что позволяет поддерживать строгий контроль ИБ в сложных и распределенных сетях. Такая интеграция автоматизации с принципами ZTA необходима для создания устойчивой системы ИБ, способной реагировать на меняющийся ландшафт угроз.

1.1.4 Автоматизация процессов обеспечения информационной безопасности

С ростом объема и сложности атак традиционные ручные методы управления ИБ, обнаружения угроз ИБ и реагирования на них уже недостаточны. Автоматизация в первую очередь направлена на снижение зависимости от ручных процессов повторяющихся и трудоемких задач. Благодаря этому защитники могут получить ряд ключевых преимуществ [7]:

1. Улучшенное обнаружение угроз и реагирование на них. Автоматизированные системы могут непрерывно отслеживать сетевой трафик, поведение пользователей и действия системы, выявляя аномалии и потенциальные угрозы в режиме реального времени. Это позволяет незамедлительно принимать ответные меры, например, изолировать взломанные сегменты ИС или блокировать вредоносный трафик, что сокращает время, необходимое злоумышленнику для использования уязвимостей, и сводит к минимуму потенциальный ущерб.

2. Повышенная эффективность и масштабируемость. По мере роста и усложнения ИТ-среды увеличивается объем событий ИБ и генерируемых данных. Автоматизация позволяет защитникам эффективно обрабатывать эти данные, обеспечивая своевременное выявление и устранение угроз ИБ. Автоматизированные инструменты могут масштабироваться вместе с ростом ИС, обеспечивая последовательное покрытие ИБ в больших и распределенных сетях.

3. Сокращение числа человеческих ошибок. Человеческие ошибки являются значительным фактором многих нарушений ИБ. Автоматизация снижает вероятность таких ошибок, обеспечивая последовательное применение политик безопасности и немедленное и точное реагирование на инциденты. Такая последовательность крайне важна для поддержания надежной системы ИБ.

Автоматизация играет важную роль в обеспечении активной защиты, предоставляя инструменты, необходимые для обнаружения, анализа и реагирования на угрозы ИБ в режиме реального времени.

1.1.5 Концепция активного и пассивного подхода к защите информации

Изначально стратегии ИБ, например, как DiD, были направлены на создание эшелонов против известных угроз. Для реализации данных стратегий были созданы МЭ, САВЗ и СОВ. Эти инструменты используются на основе уже существующих сигнатур и правил для обнаружения и реагирования на атаки. Данные стратегии объединены в группу пассивного подхода.

Однако с развитием угроз ИБ, которые становились все более изощренными и разнообразными, стали очевидны ограничения пассивных стратегий. СЗИ, используемые в рамках пассивной защиты, реагируют на угрозы после их обнаружения или совершения атаки. Такой подход делает их менее эффективными против уязвимостей "нулевого дня", APT и других видов атак, которые не следуют известным шаблонам. В результате стратегии пассивной защиты часто позволяют злоумышленникам проникать в ИС до начала ответных действий, что приводит к более значительному ущербу.

Активный подход подразумевает проактивный и динамичный подход к ЗИ, при котором защитники не только укрепляют периметры ИС, но и напрямую взаимодействуют с злоумышленником, чтобы обнаруживать, сдерживать и пресекать атаки в режиме реального времени. Подход к активной защите строится на следующих принципах [8].

Во-первых, это разведка угроз и ситуационная осведомленность. Активный подход начинается с получения и применения разведданных об угрозах. Это предполагает сбор подробной информации о потенциальном злоумышленнике, включая его тактику, технику и средства. Поддерживая высокий уровень ситуационной осведомленности, защитники могут предвидеть вероятные атаки и соответствующим образом адаптировать свои защитные стратегии. Такая проактивная позиция позволяет защитникам выявлять и понимать угрозы до того, как они полностью реализуются.

Во-вторых, это вовлечение и взаимодействие с злоумышленником. Одним из наиболее спорных аспектов активной защиты является идея прямого взаимодействия со злоумышленником. Как правило, взаимодействие заключается в использовании технологий ИО, которые заманивают злоумышленника в контролируемую среду, где их действия можно наблюдать и анализировать. Такое взаимодействие дает ценные сведения о применяемых тактиках, техниках и средствах и помогает защитникам лучше понять картину угроз. Кроме того, это может служить средством замедления или срыва атаки, что позволяет выиграть время для дальнейших оборонительных действий.

В-третьих, это динамическое и адаптивное реагирование. В рамках активной защиты реагирование на угрозы ИБ не статично, а адаптируется к изменяющейся ситуации. Это может включать, например, динамическое изменение конфигурации сети, развертывание контрмер в режиме реального времени, перехват вредоносного трафика и прочие действия, чтобы нарушить реализацию атаки злоумышленника.

Таким образом, активный подход предлагает более динамичный подход, позволяя защитникам предвидеть, обнаруживать и отражать угрозы в режиме реального времени. Вступая в непосредственное взаимодействие с злоумышленником, меры активного подхода не только сокращают окно возможностей для злоумышленника, но и собирают ценные сведения, которые могут использоваться в будущих защитных стратегиях.

Поскольку сложность угроз продолжает расти, полагаться только на меры пассивного подхода к защите уже недостаточно. Активный подход обеспечивает комплексную и устойчивую защиту ИТ-инфраструктуры, что делает их жизненно важным компонентом современных систем ЗИ [9].

1.1.6 Роль автоматизации в активном подходе к защите информации

Активный подход требует динамичности и оперативности, что позволяет предвидеть атаки и противодействовать им по мере их возникновения. Автоматизация процессов ИБ способствует этому.

Автоматизированные СЗИ могут непрерывно отслеживать сетевой трафик, поведение пользователей и системные журналы для выявления аномалий и потенциальных угроз. Эти СЗИ могут обрабатывать огромные объемы событий гораздо быстрее, чем аналитики, выявляя подозрительные и отмечая их для немедленного расследования [10]. Например, системы управления событиями ИБ (SIEM, Security Information and Event Management), интегрированные с автоматизированными СЗИ, могут коррелировать данные из различных источников и обнаруживать сложные схемы атак в режиме реального времени, обеспечивая оперативное реагирование. Эти СЗИ можно адаптиро-

вать к новой информации, совершенствуя возможности обнаружения по мере изучения предыдущих инцидентов и внешних данных об угрозах.

В активной защите способность быстро реагировать на угрозы имеет важное значение. Автоматизация позволяет без участия защитников запускать предопределенные ответные действия при возникновении инцидента ИБ. Например, при обнаружении вторжения, автоматизированные СЗИ могут немедленно изолировать скомпрометированный сегмент сети, заблокировать вредоносные IP-адреса или развернуть патчи для уязвимых систем без вмешательства защитников [11].

Автоматизация значительно улучшает развертывание и управление ИО, позволяя динамически создавать и модифицировать ложные компоненты. При ручной настройке поддержание реалистичных и эффективных ложных целей может быть трудоемким и подверженным человеческим ошибкам. Автоматизированные СЗИ могут непрерывно контролировать сетевое окружение и в режиме реального времени изменять характеристики приманок. Такая динамичность очень важна для того, чтобы ИО оставался убедительным для злоумышленника и адаптировался к изменениям в сети [12].

Автоматизация является неотъемлемой частью реализации динамических механизмов защиты, например MTD. Эффективность решения MTD, в которых поверхность атаки постоянно изменяется, чтобы ввести в заблуждение злоумышленника, во многом зависит от степени автоматизации. MTD могут периодически менять IP-адреса, модифицировать сетевые маршруты и изменять конфигурацию ИС, затрудняя злоумышленнику разведку и закрепление в сети. Это является важной частью активного подхода к защите, поскольку снижает вероятность успешной атаки и это возможно благодаря автоматизации [13].

Хотя автоматизация повышает эффективность системы защиты, человеческий опыт по-прежнему необходим. Аналитики ИБ должны интерпретировать результаты, полученные автоматизированными СЗИ, принимать стратегические решения и справляться со сложными угрозами, требующими зна-

ний и опыта. Наиболее эффективные стратегии активной защиты сочетают автоматизацию с квалифицированным персоналом, который может контролировать и совершенствовать автоматизированные процессы [14].

1.1.7 Внедрение активной защиты информации

Переход от пассивного подхода к защите к активному включает в себя несколько критически важных шагов, каждый из которых играет решающую роль в повышении общего уровня ИБ [15].

Первым шагом в реализации активного подхода является проведение комплексной оценки текущего состояния ИБ. Эта оценка должна включать в себя [16]:

1. оценка уязвимостей;

2. анализ рисков;

3. моделирование угроз.

После завершения оценки вторым шагом является интеграция передовых средств обнаружения угроз в ИС [17]. Эти инструменты составляют основу активного подхода, обеспечивая мониторинг и реагирование в режиме реального времени:

1. системы обнаружения и предотвращения вторжений (Intrusion Detection and Prevention Systems, IDPS);

2. решения для обнаружения и изучения вредоносной активности на конечных точках (Endpoint Detection and Response, EDR);

3. системы управления событиями ИБ (Security Information and Event Management, SIEM);

4. системы оркестрации, автоматизации и реагирования в ИБ (Security Orchestration, Automation, and Response, SOAR);

5. платформы анализа угроз (Threat Intelligence Platforms, TIP).

Третьим шагом является автоматизация процессов обеспечения ИБ. Автоматизация играет важную роль в активном подходе, позволяя защитникам реагировать на угрозы в режиме реального времени, снижая вероятность нанесения ущерба. Автоматизация включает в себя [18]:

1. реагирование на инциденты;

2. разработка плейбуков и оркестровка;

3. адаптивные механизмы ЗИ.

Защитникам следует внедрять автоматизированные механизмы реагирования, которые позволяют изолировать пораженные сегменты ИС, завершать вредоносные процессы и блокировать скомпрометированные учетные записи без их вмешательства. Эти автоматизированные действия сокращают время реагирования на инциденты ИБ и ограничивают поверхность атаки.

Очень важно разработать плейбуки по реагированию на инциденты ИБ, в которых описаны процедуры на распространенные сценарии атак. Эти плейбуки должны быть интегрированы с SOAR, которые автоматизируют выполнение этих процедур на основе заранее определенных критериев.

Автоматизация также должна включать адаптивные меры, которые настраивают защиту в ответ на обнаруженные угрозы. Например, при обнаружении определенного типа атаки система ИБ может автоматически повысить чувствительность определенных инструментов мониторинга или развернуть дополнительные ресурсы для защиты критически важных активов.

Четвертым шагом является создание квалифицированной команды ИБ. Хотя автоматизация является важнейшим компонентом активного подхода, человеческий опыт остается незаменимым [19]. Организации должны инвестировать в создание квалифицированной команды ИБ, способной:

1. находить угрозы и уязвимости, которые остались незамеченными автоматизированными средствами;

2. реагировать на инциденты, локализовать их и расследовать, в том числе осуществлять восстановление после инцидента, а также предпринимать действия по предотвращению будущих инцидентов;

3. постоянно обучаться и развиваться, быть в курсе последних угроз и стратегий защиты.

Пятым шагом является создание обратной связи для непрерывного совершенствования. После инцидента необходимо проводить анализ, чтобы по-

нять тактику атаки, эффективность ответных мер и пробелы в защите [20]. Полученные уроки должны быть задокументированы и использованы для совершенствования существующих мер ИБ.

Кроме того, необходимы регулярные аудиты ИБ. Проведение аудитов ИБ помогает выявить новые уязвимости или изменения в ландшафте угроз, которые могут потребовать корректировки стратегии ИБ. Эти аудиты должны включать как технические оценки, так и анализ политик безопасности и документации. Также необходимо регулярно обновлять модели угроз ИБ и плейбуки по мере появления новых угроз и развития организации. Это гарантирует, что уровень ИБ будет соответствовать текущему ландшафту угроз, а процедуры реагирования будут соответствовать реальным угрозам [21].

Защитники, которые выполнили эти шаги и достигли определенного уровня зрелости, могут еще повысить уровень ИБ при помощи методов вовлечения и взаимодействия с злоумышленником, типа ИО и MTD.

1.2 Актуальные угрозы информационной безопасности в локальных сетях передачи данных

Актуальность угроз ИБ подчеркивается растущей частотой и масштабом атак, которые причинили значительные последствия. По мере развития ИТ-инфраструктур увеличивается поверхность атаки, предоставляя злоумышленнику все больше возможностей для использования уязвимостей.

1.2.1 Угрозы, исходящие от внешнего и внутреннего злоумышленника

СЗИ, применяемые в рамках пассивного подхода к защите, прежде всего предназначены для защиты от известных угроз путем создания эшелонов безопасности, которые необходимо преодолеть внешнему злоумышленнику. Такие СЗИ очень важны для обеспечения базового уровня ИБ, но их эффективность ограничена перед сложными и новыми атаками [22]. «Статический» характер этих СЗИ также означает, что они могут не обнаружить или не отреагировать на угрозы, которые быстро изменяются или развиваются, а также в основе которых лежат нестандартные методы. В результате защитники, пола-

гающиеся только на эти СЗИ, могут с тем, что злоумышленник сможет оставаться незамеченным в сети в течение длительного времени. Это может привести к значительному ущербу, включая утечку данных, финансовые потери и репутационный вред.

Угрозы, исходящие от внутреннего злоумышленника, особенно опасны, поскольку в них участвуют доверенные субъекты. В отличие от внешнего злоумышленника, внутреннему не нужно преодолевать защиту внешнего «периметра»: он уже обладает некоторыми разрешениями необходимыми для работы с внутренними системами. Такой доступ позволяет ему обходить многие меры ИБ, что усложняет обнаружение и реагирование на его действия.

Несмотря на то, что защитники выстраивают систему защиты внешнего сетевого «периметра», злоумышленники находят недостатки и уязвимости в ней, в результате чего преодолевают её. Компания Positive Technologies в своей аналитике за 2020 год [23] приводит следующую статистику на этот счет:

1. в рамках внешнего тестирования на проникновение различных компаний в 92 % случаев был получен доступ к их локальной вычислительной сети;

2. в 100 % случаев злоумышленник может подключиться к корпоративным беспроводным сетям;

3. в 63 % систем через беспроводные сети получен доступ к ресурсам локальных вычислительных сетей.

В 2019 году Positive Technologies отметила [24], что в 92 % компаний в рамках тестирования на проникновение был получен доступ к внутренней локальной вычислительной сети из внешней, а в 100 % – был получен контроль над инфраструктурой от лица внутреннего нарушителя. Большинство предприятий не могут противостоять злоумышленнику, который проник внутрь локальной вычислительной сети.

Компания Verizon приводит данные [25] о том, что фишинг, эксплуатация уязвимостей, кража и использование учетных данных являются основными способами получения доступа в ИС организации злоумышленником.

Несмотря на то, что число инцидентов, связанных с внутренним злоумышленником, составляет всего 19 %, а с внешним – 83 %, внутренний злоумышленник может причинить значительно бóльший ущерб. При этом инциденты, которые имеют отношение к злоупотреблению доступом, обнаруживаются лишь спустя несколько месяцев или лет после их возникновения [26].

1.2.2 Тенденции к переходу на активный подход к защите

Внедрение СЗИ, применяемых в рамках активного подхода, в систему защиты может значительно расширить возможности защитников, зачастую тем самым повышая эффективность системы защиты на значительную величину. Хотя конкретные показатели могут варьироваться в зависимости от типа развернутых СЗИ, исследования и аналитические отчеты показывают, что защитники, использующие активный подход в своей стратегии защиты, отмечают заметные улучшения как по времени обнаружения и реагирования, так и в плане общей устойчивости ИС к атакам.

Например, согласно аналитическим отчетам, организации, использующие проактивные меры ИБ, такие как поиск угроз в реальном времени и ИО, могут сократить время обнаружения взлома в среднем с более чем 200 дней до нескольких дней или даже часов [27]. Такое сокращение времени обнаружения крайне важно, поскольку чем дольше угроза остается необнаруженной, тем больший ущерб она может нанести.

Системы активной защиты могут значительно повысить способность защитников предотвращать атаки по сравнению со стратегиями пассивной защиты [28]. Это обусловлено динамической природой применяемых СЗИ, которые не только реагируют на известные угрозы, но и противодействуют потенциальным атакам еще до их возникновения.

Несмотря на то, что точное улучшение может зависеть от конкретных используемых технологии и ландшафтов угроз, сообщество ИБ сходится во мнении, что СЗИ, применяемые в рамках активного подхода, значительно повышают эффективность системы защиты ИС, делая её гораздо более эффективной в обнаружении угроз и реагировании на них.

1.2.3 Нормативно-правовое регулирование активного подхода к защите

Переосмысление перестраивания системы защиты в сторону активного подхода также находит свое отражение в нормативно-правовых документах и лучших практиках. В результате анализа нормативно-правовых документов [29-34], общих [35-40] и отраслевых [41-43] стандартов в области ИБ, лучших практик [44-46] и научно-исследовательских работ ведущих университетов [47-49] получен следующий перечень базовых мер по защите локальных сетей передачи данных:

1. Обеспечение ЗИ при ее передаче, в том числе и при помощи криптографических СЗИ.

2. Обеспечение доверенных каналов и маршрутов.

3. Контроль и управление сетевыми потоками.

4. Контроль и защита конфигураций сетевого оборудования.

5. Отключение неиспользуемых и замена устаревших сервисов, служб, ресурсов и протоколов локальной сети передачи данных.

6. Изменение стандартных портов сетевых сервисов и служб.

7. Идентификация устройств и взаимная аутентификация сторон взаимодействия.

8. Мониторинг локальной сети передачи данных, регистрация событий, обнаружение и реагирование на инциденты.

9. Контроль и обеспечение подлинности сетевых соединений.

10. Контроль и разграничение доступа к ресурсам локальной сети передачи данных.

11. Выявление, анализ и блокирование скрытых каналов передачи информации.

12. Разбиение локальной сети передачи данных на сегменты и обеспечение защиты периметров сегментов.

13. Единая точка входа в локальную сеть передачи данных.

14. Наличие демилитаризованной зоны.

15. Межсетевое экранирование, в том числе и на конечных устройствах.

16. Обнаружение и предотвращение вторжений, в том числе и на конечных устройствах.

17. Защита беспроводных соединений.

18. Защита периметра локальной сети передачи данных при взаимодействии с внешними сетями.

19. Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.

20. Создание ложных компонентов, предназначенных для обнаружения, регистрации и анализа действий злоумышленников.

21. Сокрытие данных или навязывание ложных данных об архитектуре, характеристиках и технологий локальной сети передачи данных.

Как видно из перечня, регуляторы, организации и исследователи предлагают меры активного подхода в рамках комплексной стратегии ИБ.

Регулирующие органы все чаще выступают за интеграцию мер активного подхода, подчеркивая важность обмена данными об угрозах. Согласно этим предложениям, организации должны не только собирать и анализировать данные об угрозах, но и активно делиться ими с коллегами и соответствующими регулирующими органами, чтобы создать более информированную и устойчивую сеть защиты. Участвуя в обмене данными об угрозах, организации могут проактивно корректировать свою защиту на основе информации о возникающих угрозах в режиме реального времени.

Регуляторы в области ИБ также начали одобрять использование ИО. Технологии ИО все чаще рассматриваются как ценные инструменты, позволяющие защитникам взаимодействовать с злоумышленником и анализировать его тактику, не подвергая опасности реальные активы.

Непрерывный мониторинг и поведенческая аналитика являются важнейшими компонентами активного подхода, за применение которых все чаще выступают регулирующие органы. Такие нормативные документы, например, как стандарт ГОСТ Р ИСО/МЭК 27001 [35] и его международный аналог, а

также стандарт NIST [39], подчеркивают необходимость внедрения защитниками СЗИ, способных непрерывно отслеживать сетевой трафик и поведение пользователей на предмет аномальной активности. Эти меры позволяют защитникам обнаруживать угрозы и реагировать на них в режиме реального времени, и полагаться не только на анализ ситуации после возникновения инцидента.

Некоторые регулирующие органы включили меры активного подхода в перечень обязательных. Например, Общий регламент по защите данных в Европейском союзе подчеркивает необходимость быстрого обнаружения и реагирования на инциденты ИБ [34]. Это привело к появлению рекомендаций по включению СЗИ, применяемых в рамках активного подхода, таких как поиск угроз в режиме реального времени и автоматизированные механизмы реагирования.

1.3 Технология информационного обмана

ИО в ИБ подразумевает создание ложной информации, среды и компонентов, призванных привлечь, обнаружить и ввести в заблуждение злоумышленника. В отличие от традиционных мер ИБ, которые направлены на создание эшелонов безопасности, ИО предназначен для активного манипулирования злоумышленником, обеспечивая тем самым стратегическое преимущество. ИО используется для создания убедительной, но фиктивной среды, которая кажется частью реальной сети, но является изолированной и контролируемой защитниками. Такие технологии, как honeypot, honeynet, honeytoken и другие, которые также называют ложными компонентами, предназначены для привлечения злоумышленников в контролируемую среду, где их тактику можно наблюдать и анализировать, не представляя риска для реальной сети [136].

1.3.1 Типы технологии информационного обмана

Типы технологии ИО [63]:

1. Honeypot, honeywall и honeynet. Honeypot – это система-обманка, имитирующая реальный объект в сети. Она предназначена для того, чтобы заманить злоумышленника и заставить его взаимодействовать с ней, предоставляя защитникам возможность наблюдать за поведением и тактикой злоумышленника. Сети Honeynet расширяют эту концепцию, создавая целую сеть систем-обманок, что еще больше повышает достоверность и сложность ИО. А honeywall – это средство, которое используется для сбора, хранения, контроля и анализа сетевого трафика, а также перенаправления злоумышленника на системы-обманки. Как правило, honeywall размещается между реальной и ложной сетью, выступая в качестве шлюза, отделяющего обманки от остальной сети.

2. Ложные данные и honeytoken. Ложные данные подразумевают размещение в сети неверной информации, которая кажется ценной, но на самом деле является ловушкой для злоумышленника. Особым примером обманных данных является honeytoken – фрагмент информации, например, поддельные учетные данные, документы или API-ключи (Application Programming Interface, интерфейс программирования приложения). Обращение к ним демаскирует злоумышленника. Эти инструменты эффективны для обнаружения как внутренних, так и внешних злоумышленников, которые проникли за периметр и ищут ценную для себя информацию.

3. Ложные компоненты. Ложные системы и поддельные службы копируют реальные компоненты ИТ-инфраструктуры, но располагаются изолированно от основной сети. Когда злоумышленник взаимодействует с ними, он раскрывает свое присутствие и намерения, позволяя защитникам отреагировать на ситуацию до того, как будет нанесен реальный ущерб.

4. Ложный сетевой трафик. Ложный сетевой трафик подразумевает создание выглядящего достоверно, но поддельного сетевого трафика, имитирующего нормальную работу сети. Такой трафик может использоваться для введения злоумышленника в заблуждение относительно истинной природы

сети и для траты его ресурсов, заставляя его действовать на основе ложной информации.

Сочетание этих перечисленных типов технологий с автоматизацией их развертывания, реконфигурирования и масштабирования, песочницей, а также непрерывным мониторингом и анализом собранных данных образует платформу для создания распределенной инфраструктуры ложных целей (Deception Disturbed Platform, DDP) [64].

1.3.2 Платформа для создания распределенной инфраструктуры ложных целей

DDP представляет собой передовую технологию ИБ, использующую принципы ИО для введения в заблуждение, обнаружения и реагирования на угрозы ИБ. В отличие от традиционных защитных мер, которые сосредоточены на защите периметра и известных угрозах, DDP активно взаимодействует с злоумышленником, создавая среду, наполненную ложными элементами, такими как системы-обманки, поддельные данные и вводящий в заблуждение сетевой трафик, которые выглядят как настоящие объекты ИС. Эти ложные компоненты распределяются по всей ИС, создавая слой ИБ, который сбивает злоумышленника с толку, собирает оперативную информацию и повышает эффективность обнаружения и реагирования на угрозы ИБ.

DDP распределяет системы-обманки, поддельные данные и другие ложные компоненты по всей сети, а не концентрирует их в одном сегменте. Такое повсеместное развертывание гарантирует, что злоумышленник столкнется с ИО независимо от того, где он проникнет в сеть. Цель состоит в том, чтобы создать среду, в которой на каждом шагу злоумышленник потенциально может взаимодействовать с обманкой, что повышает вероятность его обнаружения.

В отличие от других технологий ИО, которые могут стать менее эффективными со временем, когда злоумышленник научится их распознавать, DDP предполагает динамическое и адаптивное развертывание ложных компонентов. Автоматизированные системы, включенные в DDP, постоянно изменяют

характеристики ложных компонентов, например, меняют их конфигурацию, IP-адреса или даже предоставляемые ими ресурсы. Благодаря такой адаптации ИО остается надежным и эффективным, не позволяя злоумышленнику легко распознать или обойти системы-обманки [65].

Еще одним преимуществом DDP является возможность сбора информации о поведении злоумышленника. Когда злоумышленник взаимодействует с ложными компонентами, DDP регистрирует их действия, инструменты и методы. Эти данные особенно ценны для понимания возникающих угроз и могут быть использованы для усиления мер ИБ. Более того, анализируя поведение злоумышленника в режиме реального времени, DDP может адаптировать ИО для более эффективного противодействия конкретным используемым тактикам [66].

Важной особенностью DDP является способность автоматизировать реакцию на обнаруженные вторжения. Например, если злоумышленник взаимодействует с ложным компонентом, DDP может автоматически изолировать скомпрометированный сегмент сети, развернуть дополнительные ложные компоненты или инициировать анализ для оценки масштабов вторжения. Такая возможность автоматического реагирования сокращает время на локализацию вторжения и минимизирует потенциальный ущерб от него [67].

Еще одним преимуществом DDP является способность обнаруживать угрозы ИБ на ранних стадиях модели Cyber Kill Chain. Поскольку ложные компоненты разбросаны по всей сети, злоумышленник, скорее всего, столкнется с ними на этапе разведки. Такое раннее обнаружение особенно ценно против APT-атак и инсайдерских угроз, которые могут оставаться незамеченными в течение длительного времени [68].

DDP работает таким образом, чтобы не нарушать работу легитимных пользователей. Ложные компоненты разработаны таким образом, чтобы быть неотличимыми от реальных объектов с точки зрения злоумышленника, но при этом не мешать нормальной работе сети. Это позволяет защитникам по-

высить уровень ИБ, не влияя на производительность и удобство работы пользователей [69].

Далее, в таблице 1, рассмотрим, как именно DDP соотносится с моделью Cyber Kill Chain для противодействия атакам злоумышленника на отдельных ее стадиях [66-69].

Таблица 1 – Действия DDP по противодействию различным стадиям реализации атаки в соответствии с моделью Cyber Kill Chain

№	Стадия реализации атаки	Предпринимаемые действия по противодействию
1	Разведка	DDP могут существенно затруднить разведку, создавая ложные компоненты, которые выглядят как цели. Когда злоумышленник исследует сеть, он сталкивается с этими компонентами, которые имитируют реальные объекты. Взаимодействие с ними предупреждает защитников о разведке, обеспечивая таким образом раннее оповещение о потенциальной атаке. Вводя злоумышленника в заблуждение на этапе разведки, DDP не позволяет им собрать достоверные данные, вынуждая их тратить ресурсы и время на ложные. Это повышает вероятность обнаружения злоумышленника и снижает вероятность его успешной атаки.
2	Вооружение	Хотя DDP сосредоточена на активном взаимодействии при помощи ложных компонентов, она может косвенно влиять на стадию вооружения. Например, предоставляя злоумышленнику ложную информацию во время разведки, DDP может заставить их создать или использовать инструменты, которые неэффективны в реальной среде.
3	Доставка	DDP разворачивает ложные компоненты, которые могут привлечь ВПО злоумышленника. Эти компоненты могут быть разработаны так, чтобы имитировать взаимодействие с пользователем или поведение ИС, что побуждает злоумышленника доставлять ВПО не тем целям. Перенаправляя доставку ВПО в системы-обманки, DDP может предотвратить компрометацию реальной цели. Кроме того, перехваченное ВПО может быть проанализировано защитниками с целью понимания методов и тактики злоумышленника и подготовки к возможным будущим атакам.
4	Эксплуатация	DDP размещает системы-обманки, которые могут фиктивно обладать определенными уязвимостями. Когда злоумышленник развертывает ВПО, оно активируется в этих ложных компонентах, вызывая оповещения и позволяя защитникам изучить методы эксплуатации уязвимостей злоумышленника в контролируемой среде. Поймав стадию эксплуатации в ловушку, DDP не только предотвращает ущерб реальным активам, но и собирает важные сведения об используемых методах и средствах злоумышленника, которые могут быть использованы при создании защитных мер.

№	Стадия реализации атаки	Предпринимаемые действия по противодействию
5	Установка	Перенаправляя попытки установки на ложные компоненты, DDP не позволяет злоумышленнику закрепиться на реальных сетевых ресурсах. DDP позволяет защитникам наблюдать за процессом установки и собирать информацию, не подвергая риску ИБ настоящую ИС.
6	Управление и контроль	Ложные компоненты могут отслеживать и анализировать трафик управления и контроля, позволяя защитникам понять цели и методы злоумышленника. Эта информация может быть использована для разрушения этих каналов управления и контроля.
7	Достижение целей	Перенаправляя усилия злоумышленника на системы-обманки, DDP защищает реальные важные активы, дает ложную информацию злоумышленнику и предоставляет защитникам возможность обнаружить атаку и отреагировать на нее до того, как будет нанесен реальный ущерб.

1.3.3 Преимущества и недостатки технологии информационного обмана

Основное преимущество ИО заключается в том, что он позволяет переломить ход атаки. Контролируя среду, в которой действует злоумышленник, защитники могут собрать важные сведения о его тактиках, методах, инструментах и целях. Эта информация может быть использована для усиления защиты, улучшения обнаружения угроз и предотвращения будущих атак. Более того, поскольку технологии ИО разработаны таким образом, чтобы быть неотличимыми от реальной среды, они могут значительно увеличить время и ресурсы, необходимые злоумышленнику для достижения цели, что часто приводит к его сдерживанию [70].

Хотя методы ИО дают значительные преимущества, они не лишены трудностей. Реализация эффективного ИО требует глубокого понимания сетевой среды и потенциальных тактик злоумышленника. Компоненты ИО должны быть достаточно достоверными, чтобы обмануть злоумышленника, что требует тщательного планирования и постоянного обновления для поддержания их эффективности. Кроме того, существует риск того, что ИО будет обнаружен, и в результате он может дать обратный эффект, что заставит злоумышленника увеличить свои усилия или изменить стратегию [67].

Однако, в процессе сбора данных злоумышленник не ограничен в исследовании истинной среды. ИО лишь формирует среду так, чтобы сделать её более привлекательной для злоумышленника с точки зрения реализации им потенциальной атаки. Существует вероятность того, что злоумышленник выберет истинный объект защиты и оценить эту вероятность достаточно сложно, так как зависит она от многих факторов в каждом конкретном случае [71].

1.3.4 Обнаружение и противодействие технологии информационного обмана

Несмотря на эффективность, технология ИО не является непреодолимой. Злоумышленник, особенно тот, кто обладает развитыми навыками и ресурсами, может обнаружить и обойти ИО.

Одним из основных методов, используемых злоумышленником для обнаружения ИО, является выявление несоответствий или аномалий в ложных компонентах. Злоумышленник может обнаружить ИО, внимательно изучив среду, в которой работают ложные компоненты. Например, если ложный компонент размещен в сети там, где он не должен существовать по логике, например, в необычно изолированном или неиспользуемом сегменте, это может вызвать подозрение. Аналогично, если с ложным компонентом отсутствует типичный фоновый шум, характерный для легитимных систем, например, сетевой трафик или активность пользователей, злоумышленник может распознать его как обманку. Кроме того, наблюдая за сетевым трафиком, злоумышленник может выявить необычные схемы обмена данными, связанные с ложными компонентами. Например, ложные компоненты могут генерировать или получать сетевой трафик, который не соответствует их предполагаемой обманом роли. Если сервер, якобы обрабатывающий конфиденциальные данные, показывает небольшой трафик, но при этом активно взаимодействует с системами ИБ, он может быть идентифицирован как обманка [68].

Ложные компоненты, которые ведут себя не так, как настоящие системы, могут быть обнаружены. Например, компонент, созданный для имитации

сервера базы данных (БД), может отвечать на запросы не так, как настоящий сервер. Злоумышленник может отправлять неожиданные или необычные запросы, чтобы посмотреть, как сервер отреагирует. Если ответ отклоняется от ожидаемого, злоумышленник может понять, что взаимодействует с обманкой [63].

Поддельные учетные данные или файлы, которые являются еще одной формой ИО, могут быть выявлены при помощи тщательного анализа. Например, злоумышленник может сравнить метаданные поддельного файла с другими файлами в системе. Если файл выглядит неуместно или не имеет достоверной истории создания и изменения, его можно определить, как обманку [72].

Некоторые системы ИО оставляют идентифицируемые сигнатуры или артефакты, которые опытный злоумышленник может распознать. Например, конфигурации по умолчанию, имена файлов или порты, используемые известными системами ИО, также могут быть их явным признаком [63].

Обнаружив обман, злоумышленник может решить полностью обойти его, избегая взаимодействия с ним, чтобы не вызвать предупреждений. Затем он может сосредоточиться на поиске и атаке реальных активов в сети. Такое избирательное нацеливание может подорвать эффективность систем ИО. В некоторых случаях злоумышленник может использовать саму систему ИО. Например, злоумышленник, осознавший, что он взаимодействует с ложным компонентом, может использовать эту возможность для передачи ложной информации защитникам. Это может заставить защитников сделать неверные предположения о методах или целях злоумышленника, что фактически обернет стратегию ИО против них. Защитники должны постоянно совершенствовать свои стратегии ИО, делая их более реалистичными, динамичными и не обнаруживаемыми [67].

1.3.5 Перспективы применения технологий информационного обмана

Одним из наиболее значимых последствий применения ИО является сокращение времени обнаружения. Когда злоумышленник взаимодействует с

ложными компонентами, немедленно включается оповещение, что приводит к более быстрому обнаружению и реагированию. Исследования показали, что технологии ИО могут значительно снизить время обнаружения [73]. Автоматизация еще больше расширяет эти возможности, позволяя реагировать гораздо быстрее [74].

ИО также снижает успешность атак. Создавая обманчивую среду, наполненную ложными компонентами, ИО повышает вероятность того, что злоумышленник будет введен в заблуждение, нацелившись на фиктивные ресурсы, а не на настоящие. Такое заблуждение не только тратит время и ресурсы злоумышленника, но и снижает вероятность успешной атаки. Исследования показали, что внедрение ИО может значительно снизить количество успешных целевых атак [75]. Это обусловлено в первую очередь неопределенностью, вносимой ложными компонентами, что усложняет процесс принятия решения злоумышленником и повышает шансы на его обнаружение до того, как будет нанесен реальный ущерб.

Технологии ИО предоставляют ценные сведения об угрозах, собирая подробную информацию о методах, тактиках, инструментах и целях злоумышленника. Эффект от такой разведки можно оценить по повышению точности обнаружения и сокращению числа ложных срабатываний. Исследования показывают, что защитники, использующие ИО, повышают точность обнаружения благодаря высокоточным предупреждениям [73], генерируемыми при взаимодействии с ложными компонентами. Такое улучшение снижает количество ложных срабатываний, позволяя защитникам сосредоточиться на реальных угрозах.

Наконец, ИО способствует снижению стоимости последствий атак. Благодаря более раннему обнаружению угроз, снижению успешности атак и уменьшению времени реагирования, ИО может значительно снизить последствия. Защитники, внедрившие ИО, сообщают о снижении затрат на устранение последствий [76].

Однако, ИО не изменяет поверхность атаки настоящей сети. Несмотря на то, что ИО создает ложные компоненты, которые могут привлечь злоумышленника, реальная поверхность атаки остается неизменной. Злоумышленник по-прежнему может идентифицировать и атаковать настоящие компоненты ИС, если он сможет отличить их от ложных. Злоумышленники могут со временем распознать закономерности в развертывании ложных компонентов, что может снизить общую эффективность ИО. А MTD, которая очень часто применяется в совокупности с ИО [70], постоянно изменяет поверхность атаки за счет периодических изменений, и таким образом усложняет проведение успешных атак для злоумышленников. MTD опирается на динамичность в том числе и легитимных объектов.

1.4 Технология защиты с использованием подвижных целей

В то время как ИО направлен на обнаружение злоумышленника и сбор разведданных о нем путем прямого взаимодействия с ним, MTD нацелена на предотвращение успешных атак за счет динамичности среды. Обе технологии могут дополнять друг друга, повышая общий уровень ИБ. MTD направлена на постоянное изменение поверхности атаки путем изменения конфигурации ИС, сети, сетевых маршрутов или IP-адресов, что затрудняет злоумышленнику атаку. Такой динамический подход создает неопределенность для злоумышленника, увеличивая сложность и стоимость атаки.

1.4.1 Принципы технологии защиты с использованием подвижных целей

Основополагающая концепция MTD базируется на идее асимметричной неопределенности. Традиционные СЗИ часто предоставляют злоумышленнику статичную цель, что позволяет ему тратить неограниченное время на изучение ИС, выявление уязвимостей и планирование атак. MTD нарушает этот процесс, постоянно изменяя поверхность атаки, в результате чего делает процесс получения стабильного и долговременного представления об ИС, которую злоумышленник планирует атаковать, более сложным.

В основе MTD лежит идея создания динамически изменяемой поверхности атаки [13]. Это предполагает изменение различных параметров ИС, таких как IP-адреса, сетевые конфигурации, версии ПО и даже структуры данных, в произвольном порядке или в ответ на предполагаемые угрозы ИБ. Таким образом, MTD заставляет злоумышленника постоянно адаптировать свои тактики, повышая вероятность его ошибок или обнаружения. Эта динамический характер противопоставляется статическим СЗИ, которые в случае компрометации оказываются менее эффективными.

1.4.2 Методы технологии защиты с использованием подвижных целей

Методы MTD классифицируются по уровням, на которых они могут применяться [77]:

1. Сетевой уровень. Такие техники, как переключение IP-адресов и рандомизация маршрутов, используются для того, чтобы скрыть истинную топологию сети и затруднить злоумышленнику проведение разведки или установление постоянных соединений.

2. Прикладной уровень. Динамическая диверсификация ПО, при которой развертывается и чередуется несколько версий ПО, гарантирует, что злоумышленник не сможет полагаться на один эксплойт для компрометации ПО в сети.

3. Уровень данных. MTD может применяться на уровне данных путем внедрения методов обфускации, которые предполагают динамическое изменение формата или шифрования данных, что не позволяет злоумышленнику использовать ранее перехваченную информацию для получения новых данных.

MTD исходит из предположения, что злоумышленник настойчив и изощрен, а также способен задействовать значительные ресурсы для атаки на ИС. Поэтому цель MTD заключается не только в предотвращении атак, но и в постоянном сдерживании усилий злоумышленника, лишая его стабильности, необходимой для планирования и осуществления успешной атаки. Предполагается, что, увеличивая стоимость и сложность атак за счет постоянных из-

менений, MTD может склонить баланс в пользу защитников, даже против хорошо финансируемого и высококвалифицированного злоумышленника [78].

Далее, в таблице 2, рассмотрим, как именно MTD соотносится с моделью Cyber Kill Chain для противодействия атакам злоумышленника на отдельных ее стадиях [79-81].

Таблица 2 – Действия MTD по противодействию различным стадиям реализации атаки

№	Стадия реализации атаки	Предпринимаемые действия по противодействию
1	Разведка	На стадии разведки злоумышленник собирает информацию об атакуемой ИС, включая топологию её сети, конфигурацию устройств, сервисов и служб, потенциальные уязвимости. MTD противодействует этому, привнося неопределенность и динамичность в среду. Такие техники, как рандомизация IP-адресов, динамический DNS и частые изменения в топологии сети, затрудняют злоумышленнику точное отображение сети и идентификацию критически важных активов. Постоянно меняя поверхность атаки, MTD увеличивает вероятность того, что злоумышленник соберет устаревшую или недостоверную информацию, тем самым снижая эффективность их последующих действий.
2	Вооружение	На стадии вооружения злоумышленник готовит инструменты, необходимые для эксплуатации выявленных уязвимостей. MTD усложняет эту стадию, поскольку гарантирует, что условия, в которых инструменты злоумышленника могли быть применены, больше не существуют или изменились к моменту начала атаки. Например, если злоумышленник разрабатывает ВПО, предназначенное для эксплуатации определенной версии ПО, техники динамического преобразования ПО в MTD могут изменить программную среду. Это вынуждает злоумышленников либо постоянно адаптировать свои инструменты, либо отказаться от атаки.
3	Доставка	Стадия доставки подразумевает передачу полезной нагрузки в целевую систему. MTD противодействует этой стадии, динамически изменяя сетевые маршруты или протоколы передачи, тем самым нарушая процесс доставки. Например, рандомизация маршрутов может перенаправить трафик так, как злоумышленник не ожидает, что приведет к неудачным попыткам доставки. Кроме того, MTD также может включать ложные компоненты, которые имитируют успешную доставку, но на самом деле направляют полезную нагрузку в изолированную среду, где она может быть безопасно проанализирована.

№	Стадия реализации атаки	Предпринимаемые действия по противодействию
4	Эксплуатация	На стадии эксплуатации полезная нагрузка злоумышленника выполняется для эксплуатации уязвимости в атакуемой ИС. MTD противодействует этому, сокращая окно атаки за счет частых изменений конфигурации ИС и версий ПО. Например, применение случайных патчей или обновлений означает, что уязвимости, планируемые к эксплуатации злоумышленником, могут быть уже устранены к моменту начала эксплуатации.
5	Установка	Стадия установки включает в себя создание плацдарма в атакуемой ИС, как правило, путем установки бэкдоров или другого ВПО. MTD нарушает этот процесс, постоянно изменяя окружение, что может нарушить или полностью предотвратить вредоносные установки. Такие техники, как динамическое изменение конфигурации или частое обновление систем, позволяют нейтрализовать бэкдор до того, как он сможет быть использован. Кроме того, MTD может внедрять ложные компоненты, которые заставляют злоумышленника думать, что он успешно установил свое ВПО, в то время как на самом деле оно находится в контролируемой и изолированной среде.
6	Управление и контроль	На стадии управления и контроля злоумышленник организует каналы связи с атакуемой ИС, чтобы отдавать команды и управлять атакой. MTD усложняет эту стадию, динамически изменяя конфигурацию сети и протоколы передачи, что затрудняет поддержание надежного соединения канала управления и контроля. Такие техники, как динамическая переброска портов и протоколов, могут нарушить каналы управления и контроля, вынуждая злоумышленника тратить дополнительные ресурсы на восстановление контроля, зачастую подвергаясь повышенному риску обнаружения.
7	Достижение целей	На стадии достижения целей злоумышленник пытается осуществить утечку данных, саботаж ИС или дальнейшее боковое перемещение в ней. MTD противостоит этому, постоянно изменяя поверхность атаки, что может нарушить возможности злоумышленника по достижению целей. Например, динамические методы обфускации данных могут изменять их, делая перехватываемую информацию бесполезной. Аналогичным образом, постоянная реконфигурация сегментов сети может предотвратить боковое перемещение, ограничивая масштаб атаки.

1.4.3 Технологические достижения, лежащие в основе реализации технологии защиты с использованием подвижных целей

Благодаря некоторым технологическим достижениям стало возможным создание и применение MTD. Эти достижения обеспечивают необходимые средства, инструменты и возможности для динамического изменения поверхности атаки. Ниже перечислены ключевые технологические достижения, которые сделали MTD осуществимой и эффективной.

1. Виртуализация и контейнеризация. Технология виртуализации позволяет создавать на одном физическом сервере несколько виртуальных машин, каждая из которых работает независимо. Эта возможность очень важна для MTD, поскольку позволяет быстро и часто изменять конфигурацию системных сред. Например, виртуальные машины можно перемещать, клонировать или развертывать с различными конфигурациями в режиме реального времени, что усложняет реализацию атаки злоумышленника. А контейнеризация, в свою очередь, позволяет запускать приложения в изолированных средах со всеми необходимыми зависимостями. Контейнеры можно динамически оркестровать, масштабировать и реконфигурировать на разных узлах, что способствует динамичности, необходимой для MTD. Контейнеры также можно легко уничтожать и воссоздавать, что еще больше усложняет попытки злоумышленника выбрать цель атаки [82].

2. Программно-определяемые сети (Software-Defined Network). SDN представляет собой серьезный шаг в управлении и эксплуатации сетевой архитектуры. Традиционные сети опираются на фиксированные, аппаратные конфигурации, которые злоумышленникам относительно легко установить и использовать в своих целях. SDN отделяет плоскость управления от плоскости данных, позволяя сетевым администраторам управлять потоками сетевого трафика программно. В контексте MTD SDN можно использовать для динамического изменения сетевых маршрутов, IP-адресов и других параметров сетевого уровня. Эта возможность особенно ценна для предотвращения разведки и перемещения в сети. Злоумышленник, пытающийся составить карту сети или установить каналы связи, может столкнуться с тем, что его усилия окажутся безуспешными, поскольку топология сетевого уровня и конфигурация сети в целом неожиданно для него изменятся [83].

3. Облачные вычисления и гибкая инфраструктура. Облачные вычисления обеспечивают гибкость и масштабируемость, необходимые для MTD, предоставляя доступ к широкому спектру вычислительных ресурсов по требованию. Облачные платформы позволяют потребителям динамически по-

треблять и освобождать ресурсы, эффективно создавая среду с подвижными целями. Гибкая инфраструктура, которая является ключевой особенностью облачных вычислений, позволяет автоматически увеличивать или уменьшать ресурсы в зависимости от нагрузки. Эта гибкость может быть использована в техниках MTD для частого перемещения нагрузок между различными виртуальными машинами, центрами обработки данных или географическими точками, что затрудняет злоумышленнику предположение и определение местонахождения критически важных активов [84].

4. Искусственный интеллект и машинное обучение. ИИ и МО играют важнейшую роль в автоматизации и оптимизации стратегий MTD. Эти технологии можно использовать для прогнозирования потенциальных векторов атак, оценки эффективности текущей защиты и автоматического инициирования изменений поверхности атаки. Например, алгоритмы МО могут анализировать сетевой трафик для выявления аномального поведения, свидетельствующего о готовящейся атаке. После обнаружения аномалии системы на базе ИИ могут автоматически перенастраивать IP-адреса, маршруты или даже развертывать узлы в сети и все это в режиме реального времени [85].

5. Передовая криптография. Криптографические достижения также способствуют MTD, позволяя использовать такие техники, как динамическое шифрование, при котором ключи или алгоритмы, используемые для шифрования данных, часто меняются. Таким образом, злоумышленнику становится сложнее расшифровать информацию, даже если им до этого удалось ее перехватить. Такие технологии, как гомоморфное шифрование, позволяющее выполнять вычисления с зашифрованными данными без их расшифровки, добавляют дополнительные уровни безопасности, которые дополняют стратегии MTD [86].

6. Реконфигурируемое оборудование и программируемые логические интегральные схемы (ПЛИС). Реконфигурируемое оборудование, в частности ПЛИС, позволяет изменять конфигурацию аппаратной логики после развертывания. В рамках MTD, ПЛИС можно перепрограммировать для изменения

обработки команд, использования памяти или протоколов, тем самым внося вариативность на аппаратном уровне. Такая динамическая реконфигурация усложняет задачу злоумышленнику по прогнозированию и использованию уязвимостей, связанных с аппаратным обеспечением, поскольку базовое поведение оборудования может меняться непредсказуемо [87].

1.4.4 Преимущества технологии защиты с использованием подвижных целей

В результате анализа публикаций [77-94] был выделен ряд преимуществ MTD. Одно из самых значительных преимуществ MTD – это повышенная сложность, которую она создает для злоумышленника. В статической ИС, обнаружив уязвимость, злоумышленник может использовать ее до тех пор, пока она не будет устранена. MTD постоянно изменяет поверхность атаки, динамически меняя конфигурацию системы, IP-адреса, сетевые маршруты или программное окружение. Эти постоянные изменения заставляют злоумышленника неоднократно адаптировать свои тактики, что увеличивает время и средства, необходимые для проведения атаки. Такая сложность может отпугнуть менее настойчивого и сбить с толку даже самого опытного злоумышленника.

MTD эффективно сокращает окно атаки для злоумышленника. Поскольку окружение постоянно меняется, время, в течение которого можно использовать уязвимость, значительно сокращается. Например, если злоумышленник обнаружит уязвимость в ПО, ПО может быть переконфигурировано или обновлено до того, как злоумышленник сможет использовать эту уязвимость. Такое сокращение окна атаки помогает минимизировать потенциальный ущерб от атаки и повышает вероятность того, что атака будет обнаружена и предотвращена до того, как она сможет нанести значительный ущерб.

MTD является ярким представителем СЗИ, применяемых в рамках активного подхода. Традиционные меры ИБ часто направлены на обнаружение атак и реагирование на них после того, как они произошли. В отличие от них, MTD разрушает потенциальные вектора атак до того, как они могут быть

полностью реализованы. Постоянно изменяя поверхность атаки, MTD снижает эффективность разведывательных действий злоумышленника, затрудняя сбор информации, необходимой для успешной атаки. Такой упреждающий подход помогает нейтрализовать угрозы до того, как они реализуются, обеспечивая более надежную и устойчивую защиту.

Уязвимости «нулевого дня», которые заранее неизвестны защитникам, представляют особую проблему для традиционных систем ИБ, поскольку они полагаются на обнаружение прежде всего по сигнатурам. MTD обеспечивает защиту от уязвимостей «нулевого дня», постоянно изменяя среду, что затрудняет злоумышленнику разработку и использование этих уязвимостей. Даже если уязвимость «нулевого дня» существует, динамическая природа MTD может смягчить ее воздействие, изменяя условия, при которых уязвимость может быть использована, тем самым ограничивая возможности злоумышленника.

MTD также предлагает преимущества в борьбе с внутренними угрозами. Внутренний злоумышленник, имеющий легитимный доступ к ИС, может хорошо разбираться в ее конфигурации и мерах безопасности. MTD может подорвать эти знания, часто изменяя среду, что затрудняет внутреннему злоумышленнику использование доступа к ИС. Например, динамические политики управления доступом или регулярно меняющиеся ключи шифрования могут ограничить возможности внутреннего злоумышленника по злоупотреблению своими привилегиями, снижая риск атаки по его инициативе.

Интеграция MTD с передовыми технологиями, такими как ИИ и МО, повышает ее эффективность, обеспечивая адаптивную и автономную ИБ. ИИ и МО могут использоваться для анализа шаблонов и прогнозирования потенциальных векторов атак, позволяя системам MTD корректировать конфигурацию в режиме реального времени в зависимости от возникающих угроз. Такая адаптивность делает MTD мощным инструментом перед лицом сложных и эволюционирующих угроз, обеспечивая уровень ИБ, который может совершенствоваться с течением времени.

Прерывая действия злоумышленника, MTD может также улучшить возможности защитников по обнаружению и реагированию. Динамическая природа MTD часто заставляет злоумышленника совершать ошибки или раскрывать свое присутствие, вызывая оповещения, которые не были бы активированы в статичной среде. Кроме того, поскольку MTD усложняет процесс атаки, она может замедлить злоумышленника, предоставляя защитникам больше времени для обнаружения и реагирования. Такая расширенная возможность может сыграть важную роль в предотвращении или смягчении последствий атак.

1.4.5 Недостатки технологии защиты с использованием подвижных целей

В результате анализа публикаций [77-94] был выделен также ряд недостатков MTD. Одним из наиболее существенных недостатков MTD является сложность, связанная с ее внедрением и управлением ею. Системы MTD требуют сложных инструментов и технологий для динамического изменения системных конфигураций, параметров сетевого уровня и программных сред. Такой динамический характер вносит высокий уровень сложности в ИТ-инфраструктуру, делая ее более сложной в обслуживании и управлении.

Например, постоянное изменение IP-адресов, маршрутов передачи или системных конфигураций может привести к трудностям в поиске и диагностике проблем при их возникновении. Системным администраторам требуются специальные навыки и инструменты для эффективного управления динамическими средами, что может привести к нагрузке на существующие ИТ-ресурсы и потребовать дополнительного обучения или найма специализированного персонала.

MTD может привести к значительным операционным издержкам, особенно с точки зрения производительности системы и потребления ресурсов. Частые изменения системных конфигураций или сетевых топологий, требуемые MTD, могут привести к увеличению времени обработки данных и замедлению времени отклика. Например, постоянная реконфигурация вирту-

альных машин или динамическое распределение IP-адресов могут вызвать задержки в сетевом трафике, что скажется на общей производительности и надежности ИС.

Динамичный и изменчивый характер MTD может создать проблемы совместимости, особенно в сложных средах. Различные компоненты ИТ-инфраструктуры должны работать согласованно. Однако постоянные изменения, вносимые MTD, могут привести к проблемам совместимости, когда некоторые компоненты могут плохо реагировать на частые изменения конфигурации или могут потребовать дополнительных настроек для поддержания совместимости.

Например, устаревшие системы или собственное ПО, не поддерживающие динамическую реконфигурацию, могут не интегрироваться в MTD, что приведет к проблемам в ИС или потребует дорогостоящих обновлений и модификаций.

Еще одним недостатком MTD является возможность непреднамеренного нарушения законных операций. Поскольку MTD предполагает постоянные изменения в ИТ-среде, существует риск, что эти изменения могут непреднамеренно затронуть легитимных пользователей или процессы. Например, частая смена IP-адресов может вызвать проблемы с подключением к сети для авторизованных пользователей, или динамическая реконфигурация ПО может привести к неожиданному поведению приложений, что вызовет сбои в бизнес-операциях.

Кроме того, необходимость постоянного мониторинга и обновления среды MTD для обеспечения ее эффективности увеличивает операционную нагрузку. Это может изымать ресурсы от других важных ИТ-функций, что может привести к неэффективности и увеличению расходов.

Внедрение MTD часто требует значительных финансовых вложений, как в плане первоначальной установки, так и в плане текущего обслуживания. Необходимость в специализированном программном и аппаратном обеспечении, а также в персонале для управления динамичной средой может при-

вести к увеличению операционных расходов. Кроме того, повышенная сложность и эксплуатационные расходы, связанные с MTD, могут потребовать приобретения современных инструментов мониторинга и найма квалифицированных специалистов по ИБ, что еще больше увеличит расходы.

Защитникам также может потребоваться инвестировать в резервные системы или решения для резервного копирования, чтобы снизить риск сбоев в работе, вызванных MTD, что добавляет еще больше расходов. Для небольших организаций или организаций с ограниченным бюджетом эти расходы могут оказаться непомерными, что ограничит целесообразность внедрения MTD. Этот риск особенно важен в средах, где время безотказной работы и надежность критически важны, например, в здравоохранении, финансах или критически важных отраслях инфраструктуры. В таких случаях вероятность сбоев может перевесить преимущества ИБ, которые дает MTD.

Еще одной проблемой, связанной с MTD, является сложность измерения ее эффективности. В отличие от традиционных мер ИБ, где успех часто можно оценить по количеству блокированных атак или обнаруженных угроз, успех MTD более абстрактен и поэтому его сложнее оценить. Динамическая природа MTD затрудняет оценку того, действительно ли изменения предотвращают атаки или просто усложняют среду, не обеспечивая значительных преимуществ в ИБ.

Более того, поскольку MTD предполагает постоянные изменения, бывает сложно установить четкую базовую линию для сравнения, что затрудняет оценку возврата инвестиций или обоснование текущих затрат и распределения ресурсов.

Наконец, существует риск того, что при внедрении MTD у защитников может возникнуть ложное чувство безопасности. Хотя MTD может значительно усложнить атаку, она не является ультимативным решением, гарантирующей защиту от всех угроз.

Чрезмерная зависимость от MTD без надлежащей интеграции с другими мерами ИБ, такими как обнаружение угроз и реагирование на инциденты,

может сделать ИС уязвимой перед атаками, которым удастся обойти или адаптироваться к MTD.

Защитникам необходимо осознать, что MTD наиболее эффективна, когда она используется как часть более широкой многоуровневой стратегии ИБ, включающей традиционные СЗИ и управление угрозами.

1.4.6 Обнаружение и противодействие технологии защиты с использованием подвижных целей

MTD – это активная динамическая технология ИБ, направленная на усложнение атак и смягчение их последствий путем постоянного изменения поверхности атаки. Хотя MTD значительно усложняет атаку, она не является непреодолимой для злоумышленника.

Одной из основных тактик, используемой злоумышленником для обнаружения MTD, является распознавание паттернов поведения, в частности, посредством анализа времени. MTD часто включает регулярные или полурегулярные изменения в среде. Наблюдая за средой в течение определенного времени, злоумышленник может заметить эти закономерности, определить интервалы, через которые происходят изменения, и предсказать будущее поведение. Зная это, злоумышленник может спланировать свою атаку так, чтобы они происходили сразу после изменения, что даст ему наибольшее время для эксплуатации уязвимостей до того, как произойдет следующее изменение [78].

Анализ времени особенно эффективен в средах, где изменения происходят по предсказуемому графику. Продвинутый злоумышленник может автоматизировать процесс мониторинга с помощью скриптов или алгоритмов МО, чтобы обнаруживать и адаптироваться к этим изменениям, тем самым снижая эффективность MTD [90].

Также злоумышленник может использовать передовые методы сбора отпечатков для получения подробной информации о конфигурации среды, несмотря на динамические изменения [95]. Такие техники, как измерение задержек, перехват и анализ сетевого трафика, позволяют злоумышленнику

сделать вывод о базовой структуре и поведении ИС, даже если она изменяется. Например, измеряя задержки между пакетами и анализируя изменения в трафике, злоумышленник может определить расположение серверов или маршруты передачи в сети, несмотря на смену IP-адресов и маршрутов. Аналогичным образом, используя инструменты для перехвата и анализа трафика от различных сетевых устройств, злоумышленник может определить типы используемых систем или ПО, даже если они меняются с течением времени. Эти сведения позволяют злоумышленнику адаптировать свои атаки к конкретной среде, на которую они нацелены, несмотря на наличие MTD.

Кроме того, MTD может быть реализована в централизованной схеме. Создание препятствий для центрального узла, который распространяет новые конфигурации, может вывести из строя MTD. Анализ сетевого трафика также может помочь злоумышленнику в установлении центрального узла. Децентрализованные схемы MTD лишены такого недостатка [88].

ИО, как правило, применяется совместно с MTD для введения злоумышленника в заблуждение [135]. Злоумышленник может использовать методы обнаружения и обхода ИО [63, 67, 68, 72]. Например, злоумышленник может сравнить поведение систем-обманок с поведением известных легитимных систем. Несоответствие времени отклика, необычные схемы трафика или аномалии во взаимодействии систем могут указать на наличие ложных компонентов. Кроме того, злоумышленник может использовать отпечатки среды для определения характеристик конкретных сегментов сети. Если определенный сегмент ведет себя иначе, чем остальная часть сети, или кажется слишком уязвимым, он может быть отмечен как потенциальная обманка. Избегая взаимодействия с такими сегментами, злоумышленник может сосредоточиться на настоящих целях.

Для эффективности MTD требуется её тщательная реализация. Непоследовательность в развертывании в разных частях системы может дать злоумышленнику возможность использовать слабые места. Например, если некоторые сегменты сети используют смену IP-адресов, а другие – нет, зло-

умышленник может нацелиться на статичные части сети или использовать их как точки входа для перехода в динамичные сегменты. Аналогично, если разнообразие ПО применяется только к определенным приложениям или системам, злоумышленник может сосредоточиться на менее защищенных системах, чтобы получить первоначальный доступ [96].

Злоумышленник может использовать задержки или проблемы синхронизации в самих механизмах MTD. Например, если существует задержка между моментом планирования изменений и моментом их полной реализации, злоумышленник может использовать это временное окно. Аналогично, если различные компоненты MTD, не скоординированы, например, смена IP-адресов не синхронизирована со сменой маршрутов передачи, злоумышленник может найти способ атаковать ИС в эти периоды несогласованности [78].

МО предоставляет злоумышленнику мощные инструменты для обнаружения и адаптации к MTD. Анализируя огромные объемы данных, собранных во время разведки, алгоритмы МО могут выявить закономерности в том, как реализуется MTD. Например, МО можно использовать для предсказания того, когда и как MTD изменит конфигурацию, основываясь на прошлом поведении, что позволяет злоумышленнику планировать свои действия соответствующим образом. МО также может быть использовано и для обнаружения ИО путем обучения на основе предыдущих взаимодействий. Со временем эти алгоритмы становятся все более искусными в различении реальных систем и ложных, эффективно нейтрализуя одну из ключевых компонент защиты MTD [97].

Человеческий фактор также остается значительной уязвимостью даже в средах, защищенных MTD. Сложность внедрения и управления может привести к неправильной конфигурации, нарушениям правил ИБ или непоследовательному применению методов MTD. Выявляя и используя эти слабые места, злоумышленник может обойти защиту MTD [95].

1.4.7 Перспективы применения технологии защиты с использованием подвижных целей

Оценка влияния MTD на ИБ включает в себя анализ нескольких ключевых показателей, таких как снижение успешности атак, увеличение времени компрометации ИС и общее повышение устойчивости ИС. Хотя конкретные значения могут варьироваться в зависимости от применяемых техник MTD и конкретных условий, в которых они применяются, исследования в этой области позволили получить некоторые приблизительные показатели, демонстрирующие эффективность MTD.

Исследования показали, что MTD может значительно снизить процент успешных атак. Например, исследования показывают, что MTD может снизить успешность попыток проникновения [88-90] по сравнению со статическими механизмами защиты. Такое снижение обусловлено в первую очередь повышенной сложностью и непредсказуемостью технологии, что заставляет злоумышленника постоянно адаптировать свои стратегии, и как следствие это приводит к ошибкам или его обнаружению.

Также исследователями было показано, что MTD в совокупности с ИО улучшает показатели обнаружения атак [96]. Это улучшение имеет решающее значение для сокращения времени пребывания злоумышленника в сети, тем самым ограничивая потенциальный ущерб, который он может нанести.

MTD может значительно увеличить время, необходимое злоумышленнику для компрометации ИС. Метрика, известная как окно атаки, имеет решающее значение для оценки эффективности мер безопасности. Исследования показывают, что MTD может значительно увеличить эту величину, в зависимости от частоты и характера вносимых изменений [91]. Например, в сценариях, где смена IP-адресов происходит каждые несколько минут, время, необходимое злоумышленнику для успешного исследования сети, сокращается, а время необходимое для проведения скоординированной атаки, соответственно увеличивается, что дает защитникам больше времени для обнаружения атаки и реагирования на нее.

Одним из значительных преимуществ MTD является его способность уменьшать время воздействия уязвимости. Постоянно изменяя поверхность атаки, MTD ограничивает время, в течение которого уязвимость может быть использована. Исследования показывают, что MTD может значительно сократить время воздействия известных уязвимостей [82], что значительно затрудняет злоумышленнику использование этих слабых мест до того, как они будут устранены с помощью патчей или изменений конфигурации.

Внедрение MTD значительно увеличивает ресурсы, необходимые злоумышленнику для проведения успешных атак. Исследования показали, что вычислительные и временные ресурсы, необходимые злоумышленнику для адаптации к MTD, могут значительно увеличиться по сравнению со статическими средами [93]. Это служит сдерживающим фактором, особенно для злоумышленника с ограниченными ресурсами, и заставляет его пересмотреть целесообразность атаки.

Улучшения, которые дает MTD, подчеркивают ее эффективность в повышении уровня ИБ. Снижая процент успешных атак, сокращая окно атаки, повышая уровень обнаружения, уменьшая воздействие уязвимостей и увеличивая затраты ресурсов для злоумышленника, MTD значительно повышает уровень ИБ ИС. Эти показатели свидетельствуют о том, что MTD – это не только теоретическое достижение, но и практическое развитие мер ИБ. Поскольку угрозы продолжают развиваться, внедрение MTD и связанных с ним преимуществ, вероятно, будет приобретать все большее значение для защиты критически важных инфраструктур и конфиденциальных данных.

Хотя MTD дает значительные преимущества с точки зрения ИБ, её внедрение часто связано со значительной сложностью и издержками [78]. Эта сложность может привести к проблемам в управлении ИС, совместимости ее частей и производительности. Существует необходимость в разработке новых решений MTD, которые минимизируют её недостатки, сохраняя или даже увеличивая её преимущества. Например, можно разработать облегченные методы MTD, требующие меньших вычислительных ресурсов, что сделает их

более доступными для организаций с ограниченной ИТ-инфраструктурой. Кроме того, новые автоматизированные инструменты, упрощающие развертывание и управление MTD, могут снизить нагрузку на системных администраторов.

Поскольку угрозы продолжают развиваться, решения MTD должны стать более адаптируемыми и масштабируемыми. Будущие стратегии MTD должны быть способны адаптироваться не только к текущему ландшафту угроз, но и к специфическим потребностям и характеристикам различных типов ИС. Это может включать в себя разработку модульных решений, которые могут быть адаптированы к различным отраслям, таким как финансы, здравоохранение или критическая инфраструктура, каждая из которых сталкивается с уникальными проблемами ИБ. Масштабируемые решения MTD, которые можно легко развернуть в больших распределенных сетях, необходимы, поскольку организации все больше переходят к облачным и гибридным средам [81].

1.4.8 Интеграция технологии защиты с использованием подвижных целей и технологий информационного обмана

Интеграция MTD и ИО представляет собой эффективный подход к повышению уровня ИБ организации. Обе технологии направлены на создание динамичной и непредсказуемой для злоумышленника среды, что снижает успешность атаки. В то время как MTD направлена на постоянное изменение поверхности атаки, ИО направлен на введение в заблуждение и на сбор разведданных о злоумышленнике при помощи ложных компонентов. Интеграция этих двух технологий может обеспечить значительные преимущества, повысив устойчивость и адаптивность защитных систем.

MTD и ИО должны быть развернуты скоординированно, чтобы максимизировать их эффективность. Например, когда MTD изменяет конфигурацию сети, новые ложные компоненты должны быть автоматически сгенерированы и развернуты в соответствии с обновленной средой. Это гарантирует,

что слой обмана останется актуальным, сохраняя свою эффективность в введении злоумышленника в заблуждение [96].

Для эффективной интеграции MTD и ИО они должны управляться с помощью единой платформы, обеспечивающей централизованную видимость и контроль. Эта платформа может коррелировать данные, поступающие от обеих технологий, обеспечивая комплексное представление об угрозах и координируя ответные действия. Единая платформа также упрощает управление этими сложными системами, снижая вероятность неправильной конфигурации и обеспечивая согласованную работу обеих технологий [65].

1.5 Постановка задач исследования

В условиях быстро меняющегося ландшафта ИБ традиционные стратегии пассивной защиты, такие как DiD, перестают отвечать высоким требованиям в борьбе с сложными угрозами, с которыми сегодня сталкиваются защитники. DiD, основанная на многоэшелонированной системе защиты, заключается в предположении, что злоумышленник может быть остановлен на одном из эшелонов, если он преодолел другой. Однако современные злоумышленники разработали передовые тактики, методы и инструменты, позволяющие обходить СЗИ, что делает стратегии пассивной защиты менее эффективными в борьбе с постоянными и эволюционирующими угрозами.

Признавая ограниченность стратегий пассивной защиты, защитники все чаще используют стратегии активной защиты, например, такие как ZTA. ZTA работает по принципу «никогда не доверяй, но всегда проверяй», обеспечивая аутентификацию, авторизацию и постоянную проверку каждого соединения, независимо от местоположения пользователя или его устройства. Такой подход значительно повышает ИБ, сводя к минимуму риск несанкционированного доступа и горизонтального перемещения в ИС, обеспечивая тем самым более динамичную и надежную защиту от угроз.

После того как защитники внедрили фундаментальные компоненты ZTA, они могут еще больше повысить уровень ИБ, интегрировав передовые

методы активной защиты, такие как ИО и MTD. Исследования подтверждают эффективность этих технологий с точки зрения повышения ИБ. Технологии ИО, предполагающие создание систем-обманок и ложных компонентов для введения злоумышленника в заблуждение, помогают обнаруживать угрозы на ранних стадиях атаки и собирать ценную разведывательную информацию. А MTD, с другой стороны, постоянно изменяет поверхность атаки, затрудняя злоумышленнику атаку за счет того, что атакуемая ИС постоянно изменяется. Эти технологии в совокупности с базовыми мерами ZTA создают более устойчивую и адаптивную систему ИБ, которая может лучше противостоять сложным атакам.

Несмотря на преимущества, существующие решения ИО и MTD не лишены недостатков. Такие проблемы, как сложность развертывания и эксплуатации, повышенная потребность в ресурсах и риск обнаружения злоумышленником, ограничивают их эффективность. Поэтому существует необходимость в разработке новых решений, устраняющих эти недостатки. Инновации в этих областях могут привести к созданию более удобных, масштабируемых и незаметных систем ИО и MTD, что еще больше повысит способность защитников противостоять современным угрозам. Продолжая совершенствовать эти технологии, появляется возможность обеспечить более надежную и эффективную защиту перед лицом постоянно меняющихся угроз.

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.

1.6 Выводы

1. В рамках данной главы 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.

2. 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.

3. 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.

4. 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.

5. Таким образом, диссертационное исследование является актуальным. В главе была определена цель и задачи исследования. Целью диссертационного исследования является повышение защищенности локальной сети передачи данных от стороннего исследования за счет изменения поверхности атаки.

2. Метод защиты локальной сети передачи данных от стороннего исследования на основе реконфигурации топологии сетевого уровня

2.1 Анализ объекта защиты

Важнейшим шагом в построении эффективной системы защиты является анализ объекта защиты. Этот анализ необходим для понимания уязвимостей, потенциальных угроз и мер, необходимых для эффективного снижения рисков. Без анализа объекта защиты меры ИБ могут быть неверно согласованы, что приведет к появлению пробелов в защите, которыми может воспользоваться злоумышленник.

2.1.1 Описание объекта защиты

Настоящая работа посвящена защите локальных сетей передачи данных от исследования злоумышленником. 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. Знание этой информации может позволить злоумышленнику определить критические хосты, узкие места и потенциальные уязвимости. Защита этой информации имеет важное значение для создания безопасной и устойчивой сетевой инфраструктуры. С одной стороны, статическая природа этой информации позволяет собирать её неограниченное время, а с другой стороны, злоумышленник может обладать такими знаниями и временем, что он на основе этой информации может спланировать атаку, которой защитники не смогут противодействовать.

2.1.2 Потенциальные угрозы

Наиболее значимыми угрозами ИБ в контексте защиты локальной сети передачи данных от стороннего исследования являются [98]:

1. угроза обнаружения узлов, которая заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов;

2. угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб, которая заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (сканирование портов) для получения сведений для реализации других угроз;

3. угроза определения топологии вычислительной сети, которая заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз;

4. угроза перехвата данных, передаваемых по вычислительной сети, которая заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (прослушивание трафика) режиме для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы скрытным получателем перехватываемых данных;

5. угроза определения типов объектов защиты, которая заключается в возможности проведения нарушителем анализа выходных данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе (fingerprinting);

6. угроза получения предварительной информации об объекте защиты, которая заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищённости дискредитируемой системы, её конфигурации и потенциальных уязвимостях и других сведений, путём проведения мероприятий по сбору и анализу доступной информации о системе.

Злоумышленник осуществляет исследование сети на стадии разведки согласно модели Cyber Kill Chain. Противодействие злоумышленнику на стадии разведки – это важнейший аспект эффективной стратегии ИБ, так как это может предотвратить реализацию всей атаки. Противодействуя злоумышленнику на ранней стадии, защитники могут предотвратить получение злоумышленником достаточного объема информации для планирования точной и эффективной атаки. Такие упреждающие действия значительно снижают риск полномасштабной атаки и связанный с ней потенциальный ущерб.

Актуальность потенциальных угроз подтверждается статистикой инцидентов ведущих организаций в области ИБ. Компания Positive Technologies в 2019 году установила, что как правило, на первом этапе после проникновения злоумышленник осуществляет сетевую разведку [24]. А в 2020 году отмечает,

что в 33 % компаний наблюдалось сканирование внутренней сети, а в 19 % – сбор информации [23].

Компания Ростелеком Солар в своем отчете указывает на то, что после проникновения в сеть злоумышленник выполняет её сканирование [50].

Компания Kaspersky ICS CERT установила, что APT-группировки используют инструменты для сканирования и кражи данных [51].

Статистика компании Infowatch за 2016 год говорит о том, что рост утечек данных из российских организаций связан с ростом ценности информации и увеличением числа каналов передачи данных. Наибольшее число утечек пришлось на сетевой канал – 64 % [52].

По статистике компании JSOC за 2015 год, все больший интерес для злоумышленников начинают представлять схемы сетей и особенности работы ИС, которые в дальнейшем используются при планировании и подготовке последующих атак и мошеннических схем [53].

По статистике центра мониторинга «Перспективный мониторинг» за 2017 год, около 19 % зарегистрированных событий связаны со сканированием сети [54], а уже в 2018 году отмечен рост числа событий сканирования по сравнению с 2017 годом [55].

Организация ENISA в своем отчете за 2023 год отмечает, что сканирование используется в большинстве сценариях типичных атак [56].

Компания Check Point в своем исследовании за 2023 год утверждает, что злоумышленники используют средства сетевой разведки и маскируют свою активность под легитимные сканеры уязвимостей и средства обнаружения вторжений [57].

Компания Sophos в своем отчете за 2024 год указывает следующие инструменты для сетевой разведки, которые используют злоумышленники: Advanced IP Scanner, NetScan, PCHunter, HRSword [58].

Компания Sirar в своей статистике за 2023 отмечает, что сетевое сканирование входит в топ 10 обнаруженных инцидентов [59].

Организация CPX также указывает, что сканирование/зондирование/попытки доступа занимают долю 15 % от всех обнаруженных инцидентов [60].

Компания Ivanti предсказывает, что злоумышленники будут в скором времени использовать искусственный интеллект для быстрого исследования сети и поиска уязвимостей [61].

2.1.3 Модель нарушителя

В настоящей работе рассматривается злоумышленник, который успешно получил несанкционированный доступ к локальной сети передачи данных, но сосредоточился исключительно на исследовании сети, не прибегая к деструктивным действиям. Этот злоумышленник действует изнутри сети, собирая информацию о ней для реализации точной и эффективной атаки.

Злоумышленник может сканировать сеть, чтобы обнаружить активные устройства, определить MAC-адреса и IP-адреса, а также построить топологию сети. Выполняя сканирование портов, злоумышленник может определить, какие службы запущены на различных устройствах и есть ли открытые порты, уязвимые для будущей эксплуатации.

Кроме того, злоумышленник может перехватывать и анализировать сетевой трафик для того, чтобы собирать статистические данные по обмену, отслеживать паттерны взаимодействия и извлекать прочую информацию, которая содержит детали конфигурации сети. Злоумышленник может перемещаться по сети, исследуя её.

Хотя у злоумышленника нет никаких предварительных знаний о сети, существующие методы исследования сети позволяют постепенно получить эти знания, которые могут иметь ценность для планирования дальнейшей атаки.

Исследование сети является первым шагом в более широком плане атаки, где собранная информация используется для создания эффективной целевой атаки. Несмотря на то, что злоумышленник не нарушает работу сети, его действия представляют собой значительную угрозу, поскольку получение де-

тального представления о сети может сделать будущие атаки более точными и эффективными. Для эффективного противодействия исследованию злоумышленником локальной сети передачи данных необходимо понимание его методов и средств.

2.1.4 Методы и средства реализации потенциальных угроз

Методы стороннего исследования локальной сети передачи данных можно классифицировать следующим образом [99]:

1. сканирование сети (scanning);
2. перехват и анализ сетевого трафика (sniffing):
   а) пассивный;
   б) активный.

Сканирование сети представляет собой процесс исследования сети с целью выявления активных устройств, открытых портов, служб и топологии сети. Существуют различные типы сканирования сети, каждый из которых имеет свои цели и результаты. Наиболее распространенные типы включают [100]:

1. Ping-сканирование. Этот базовый тип включает в себя отправку эхо-запросов протокола Internet Control Message Protocol (ICMP) на различные устройства в сети, чтобы определить их доступность и активность. Ping-сканирование определяет активные узлы, но предоставляет ограниченную информацию о службах, работающих на этих узлах.

2. Сканирование портов. Этот тип используется с целью обнаружения открытых портов и связанных с ними служб. Определив, какие порты открыты, злоумышленник может выяснить, какие службы запущены, и может потенциально использовать их для реализации будущих атак.

3. Сканирование служб. Это позволяет не только определить открытые порты, но и собрать информацию о типах и версиях ПО, работающего на этих портах. Это позволяет злоумышленнику искать уязвимости в конкретных версиях ПО. Злоумышленник, используя специальные запросы, может выяснить версию ПО, после чего выделить уязвимые версии при помощи различ-

ных баз данных уязвимостей. Злоумышленник может применить различные техники атак для известных служб для проверки наличия определенной уязвимости.

4. Сканирование уязвимостей. Этот тип сканирования сочетает в себе сканирование портов и служб с их поиском в известных базах данных уязвимостей. Это позволяет злоумышленнику относительно быстро обнаружить потенциальные уязвимости в сети, которые могут быть использованы в реализации будущих атак.

Сканирование сети имеет параметры конфигурации: диапазон адресов, диапазон портов, интервал опроса, глубина поиска. При помощи конфигурирования этих параметров злоумышленник может провести сканирование так, чтобы, с одной стороны, оно было эффективно с точки зрения объема полученных данных о сети и приемлемо по длительности, а с другой, чтобы злоумышленник не выдал своего присутствия в сети. Злоумышленник также может скрыть свое присутствие в сети, отправляя запросы через другой узел сети. Наиболее популярные инструменты для автоматизированного сканирования: nmap, Zmap, Masscan; для поиска уязвимостей: Burp Suite, Metasploit, OpenVAS, Tsunami, Vulners; для веб-сканирования: Skipfish, Nikto, ZAP, Acunetix, SQLmap [101].

При помощи перехвата и анализа трафика злоумышленник решает похожие задачи, что и в случае сканирования сети. Однако, перехват и анализ трафика открывают перед злоумышленником более широкие возможности: определение объема трафика, выявление маршрутов передачи трафика, сбор статистических данных по обмену, выделение паттернов взаимодействия между узлами, идентификация используемых протоколов, кража конфиденциальной информации при её передаче и так далее [102]. Так как объем собранного трафика может быть больши́м, злоумышленник, как правило, фильтрует его по протоколам, адресам, портам и другим параметрам. Даже если трафик зашифрован, злоумышленник может извлечь из него полезную информацию [103].

Пассивный перехват – это скрытое прослушивание и захват сетевого трафика без изменения или нарушения связей между узлами. Злоумышленник остается незамеченным, собирая информацию из данных, передаваемых по сети. Злоумышленник перехватывает и анализирует только тот трафик, который доступен в точке закрепления. Основные методы пассивного перехвата:

1. Прослушивание пакетов. Для прослушивания пакетов используются такие инструменты, как Wireshark и tcpdump. Эти инструменты позволяют злоумышленнику перехватывать данные, проходящие через сетевую карту скомпрометированного устройства, анализировать заголовки пакетов и проверять их содержимое [104].

2. Аппаратные устройства прослушивания сети. При пассивном перехвате иногда используются специальные аппаратные устройства, устанавливаемые на сетевые кабели для дублирования сетевого трафика и отправки его на устройство злоумышленника для анализа. Эти устройства прозрачны для ИС, что делает их удобными для перехвата без обнаружения [105].

Главное преимущество пассивного перехвата и анализа сетевого трафика – это скрытность. Поскольку злоумышленник не изменяет сетевой трафик и не взаимодействует с сетью, пассивный перехват сложно обнаружить с помощью обычных механизмов защиты сети. Это делает его очень удобным для длительного наблюдения. Поскольку пассивный перехват не предполагает вмешательства в нормальную работу сети, это позволяет злоумышленнику избежать паттернов поведения, которые могли бы предупредить защитников об его атаке [106].

Главный недостаток пассивного перехвата – это ограниченность видимым трафиком. Для эффективного перехвата злоумышленник должен иметь доступ к сетевому трафику всей сети или большей части её сегментов. Этого относительно легко добиться в слабо сегментированных сетях, однако сложно в хорошо сегментированных и изолированных [106].

Активный перехват, в отличие от пассивного, предполагает непосредственное взаимодействие с сетью и манипулирование трафиком в процессе его прохождения по сети. Активные методы более рискованны с точки зрения обнаружения, но обеспечивают большую гибкость и контроль над трафиком. Основные методы активного перехвата:

1. Атаки типа «человек посередине» (Man-In-The-Middle, MITM). Злоумышленник располагается между двумя общающимися сторонами. Затем он перехватывает трафик, возможно изменяет его и пересылает получателю без ведома обоих сторон. Реализуется данная атака при помощи: ARP-спуфинга, DNS-спуфинга, снятия SSL, прокси и других методов [107].

2. Зеркалирование трафика. Злоумышленник, получивший несанкционированный доступ к сетевому коммутатору или маршрутизатору с функцией зеркалирования, может настроить его на зеркалирование трафика целевых сегментов сети в ту точку, в которой он сможет этот трафик перехватить, что позволит ему наблюдать за всеми данными, проходящими через эти сегменты [108].

Главное преимущество активного перехвата – это более широкие возможности в отличие от пассивного. Активный перехват дает злоумышленнику возможности вводить, изменять, перенаправлять или блокировать трафик. Также он позволяет злоумышленнику проводить атаки на зашифрованный трафик, перехватывая и повторно шифруя его с помощью собственных сертификатов [106].

Однако существенным недостатком активного перехвата является повышенный риск обнаружения. Поскольку активные методы изменяют трафик или напрямую взаимодействуют с компонентами сети, их гораздо легче обнаружить. Активный перехват несет в себе риск непреднамеренного нарушения работы сети, что также может предупредить защитников об атаке [106].

2.1.5 Требования к контрмерам

Такие активные СЗИ, как ИО и MTD, увеличивающие или изменяющие поверхности атаки, могут ввести злоумышленника в заблуждение, при этом

защищая реальные активы. Внедряя ИО и MTD, защитники могут увеличить стоимость и сложность атаки для злоумышленника. Это может заставить его вообще отказаться от атаки, особенно если он считает цель незначительной для слишком сложной или дорогостоящей атаки.

Для противодействия потенциальным угрозам предлагаемый метод должен удовлетворять следующим требованиям:

1. Случайное динамическое распределение адресов. Злоумышленник обычно полагается на сканирование статических адресов и идентификации устройств. Постоянно меняя эти параметры, злоумышленнику становится сложнее отслеживать сетевые устройства.

2. Случайная динамическая реконфигурация топологии сети. Изменения логических путей, по которым проходят пакеты данных, не позволяют злоумышленнику составить карту сети.

3. Случайная маршрутизация. Злоумышленник перехватывает трафик, наблюдая за предсказуемыми шаблонами маршрутизации. Рандомизация маршрутов снижает вероятность того, что злоумышленник сможет перехватить данные.

4. Обнаружение и реагирование на действия злоумышленника. Обнаружение исследования сети в реальном времени дает возможность пресечь попытки злоумышленника собрать информацию о сети до того, как он сможет ее использовать.

5. Автоматическое восстановление работоспособности. Автоматическое восстановление работоспособности поддерживает безопасность и функциональность сети, обеспечивая предсказуемое время простоя после реконфигурации.

Реализация этих требований может защитить от исследования локальную сеть передачи данных, делая сетевую среду непредсказуемой и сложной для злоумышленника. Злоумышленник не сможет обладать долговременной информацией о сети, так как она постоянно изменяется. Как следствие, злоумышленник не сможет спланировать точную и эффективную атаку.

2.2 Формализация предлагаемого метода

Так как настоящая работа посвящена защите локальной сети передачи данных от исследования злоумышленником, следует подробно рассмотреть методы MTD сетевого уровня.

2.2.1 Методы сетевого уровня

MTD – это технология. Технология – это совокупность методов для достижения цели. Метод – высокоуровневый, систематический и структурированный способ достижения цели. Методы MTD делятся по уровням на: сетевого уровня, прикладного уровня и уровня данных. В свою очередь, методы сетевого уровня делятся на [91]:

1. Методы, направленные на изменения адресов и портов. Эти методы предназначены для снижения эффективности сканирования сети за счет того, что злоумышленник не сможет точно идентифицировать конкретные узлы и службы. Как следствие, злоумышленник не сможет сопоставить известные уязвимости с открытыми портами и с конкретными узлами сети.

2. Методы, направленные на изменения маршрутов. Эти методы предназначены для снижения эффективности составления карты сети, а также перехвата и анализа сетевого трафика. Изменения маршрутов гарантируют, что злоумышленники не смогут полагаться на фиксированные маршруты для перехвата или использования трафика.

3. Методы, направленные на изменения топологии сети. Эти методы предназначены для динамического изменения структуры сети, чтобы создать непредсказуемую среду для злоумышленника. Изменения топологии подразумевает периодическую перестройку соединений между узлами.

4. Методы, направленные на изменения узлов. Эти методы предназначены для изменения атрибутов и программной конфигурации узлов сети. Например, можно перемещать службы и сервисы между узлами сети. Как следствие, злоумышленник не сможет обладать долговременной информацией о расположении сервисов и служб.

5. Методы, направленные на динамическое распределение ресурсов. Эти методы MTD основаны на предположении, что защитники используют ограниченное количество СЗИ, и что их размещение оказывает негативное влияние на сеть. Таким образом, эти методы направлены на обеспечение близкого к оптимальному (но все же изменяющегося со временем) размещению этих СЗИ в защищаемой сети.

2.2.2 Суть и новизна предлагаемого метода

Цель предлагаемого метода – защита локальной сети передачи данных от стороннего исследования при помощи периодической замены топологии сетевого уровня (далее – реконфигурации). Это относит предлагаемый метод к классу методов, направленных на изменения топологии сети. Исходный метод данного класса представлен на рисунке 1 [77, 91, 92, 116, 117, 118, 126, 127, 128, 129], где K – порядковый номер сгенерированной сетевой топологии. Зеленым цветом выделен блок, относительно произведена модификация метода.

Блок A1 соответствует процессу инициализации сети [126]. Данный процесс контролируется администратором сети. После развертывания топологии, сеть находится в процессе сходимости. Если топология сформирована корректно, с учетом ограничений физической инфраструктуры и конкретного применяемого метода, то процесс сходимости завершиться корректно и на выходе данного процесса возникнет сетевой трафик.

Блок A2 соответствует процессу мониторинга сети [127]. Данный процесс выполняется средством мониторинга сетевого трафика. В случае, если злоумышленник присутствует в сети, в результате его действий могут возникнуть события, которые будут детектированы средством мониторинга. На выходе данного процесса формируется некоторый список узлов, которые могут быть ранжированы в соответствии с правилами мониторинга по степени опасности.

Блок A3 соответствует процессу ожидания триггера [117, 128, 129]. Данный процесс выполняется контроллером сети. В результате истечения

временного периода или оповещений СЗИ в соответствии с правилами обработки триггеров на основе данных мониторинга, полученных из блока А3, может быть инициирована генерация новой сетевой топологии с некоторыми наборов параметров, который определен каждым конкретным методом.

Блок А4 соответствует процессу генерации сетевой топологии [128]. Данный процесс выполняется контроллером сети способом, который определен каждым конкретным методом, на основе параметров, полученных из блока А3.

Блок А5 соответствует процессу развертывания сетевой топологии [77], полученной из блока А4. Данный процесс выполняется контроллером сети. Параметры сгенерированной сетевой топологии задаются элементам, образующим данную сеть.

В результате этих периодических действий, собранная информация злоумышленником частично или полностью устаревает. Злоумышленник не сможет полагаться на собранные во время исследования сети данные, так как они могли уже устареть. Так как диссертационная работа посвящена противодействию разведке, другие стадии атаки не рассматриваются.

Модификация предполагает генерацию новой топологии на основе групп в сочетании с изменением физических и логических адресов хостов сети, а также маршрутов передачи информации, что образует топологию сетевого уровня. Основная идея достижения цели метода заключается в реконфигурации топологии сетевого уровня локальной сети передачи данных. Предлагаемый метод представлен на рисунке 2.

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.

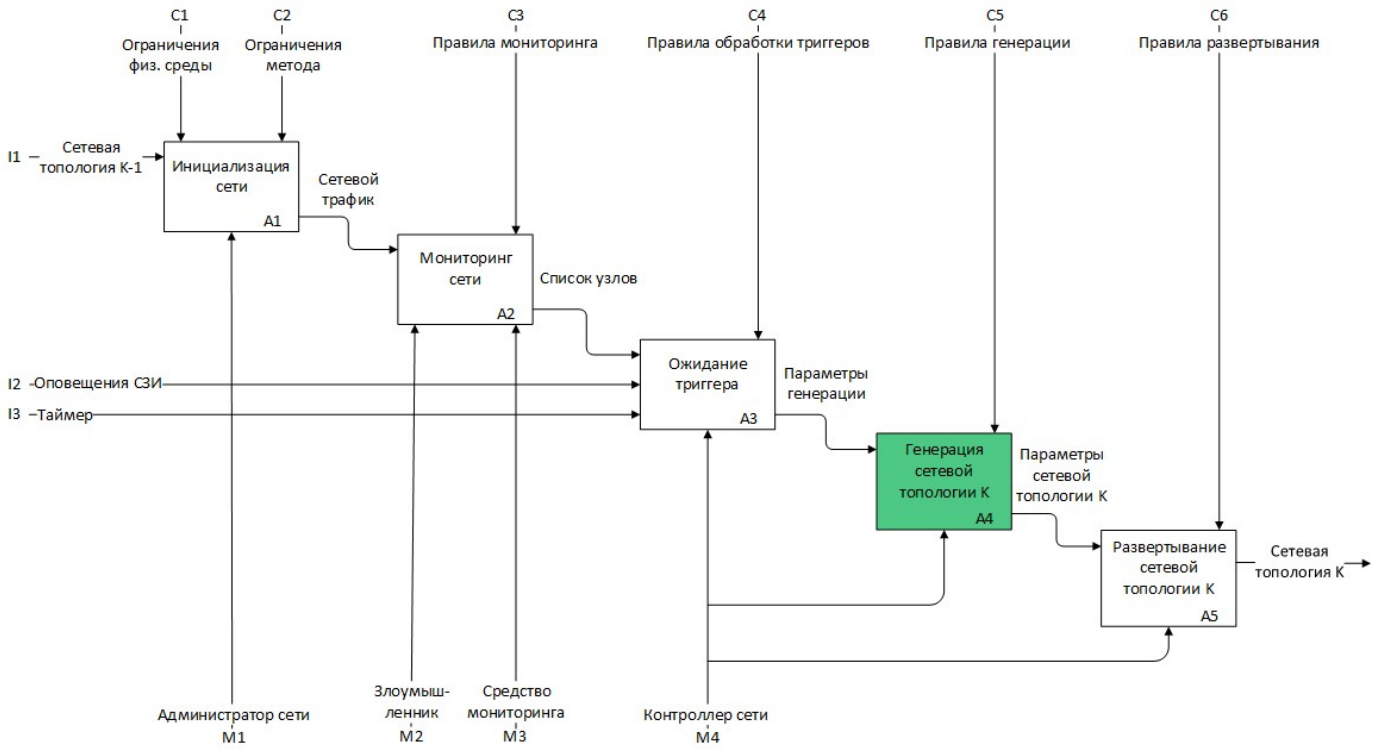

Рисунок 1 – IDEF0-диаграмма оригинального метода

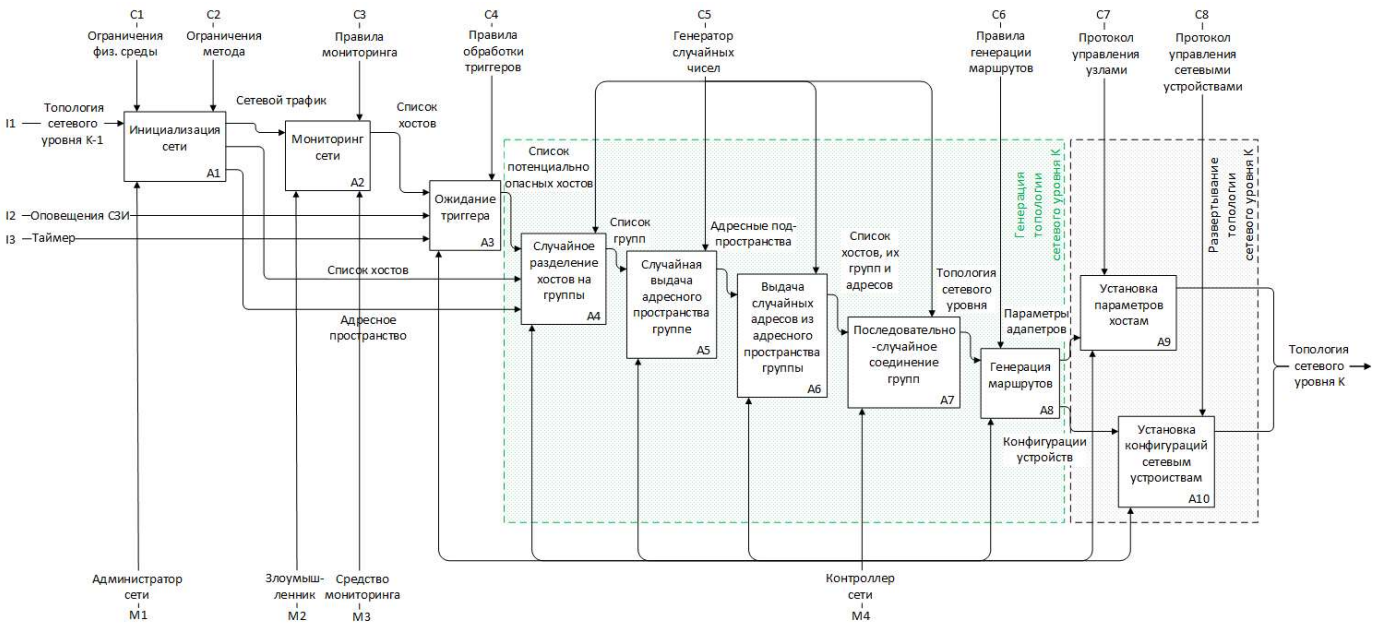

Рисунок 2 – IDEF0-диаграмма модифицированного метода

Затем эти группы последовательно-случайно соединяются между собой. Затем на основе полученной логической топологии сети генерируются маршруты. Таким образом получается новая топология сетевого уровня. При этом при формировании новой топологии из взаимодействия могут быть исключены потенциально опасные хосты, 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 каждой реконфигурации, то есть множество хостов, идентифицированных злоумышленником, становится пустым при каждой итерации метода.

Теоретический график зависимости знаний злоумышленника о системе в зависимости от времени можно представить так, как на рисунке 3 [91]. Предложенный метод является реализацией системы с синхронной реконфигурацией и неограниченным пространством реконфигураций (за счет перемешивания хостов случайным образом).

Далее необходимо провести оценку защищенности объекта защиты предложенного метода при помощи математической модели.

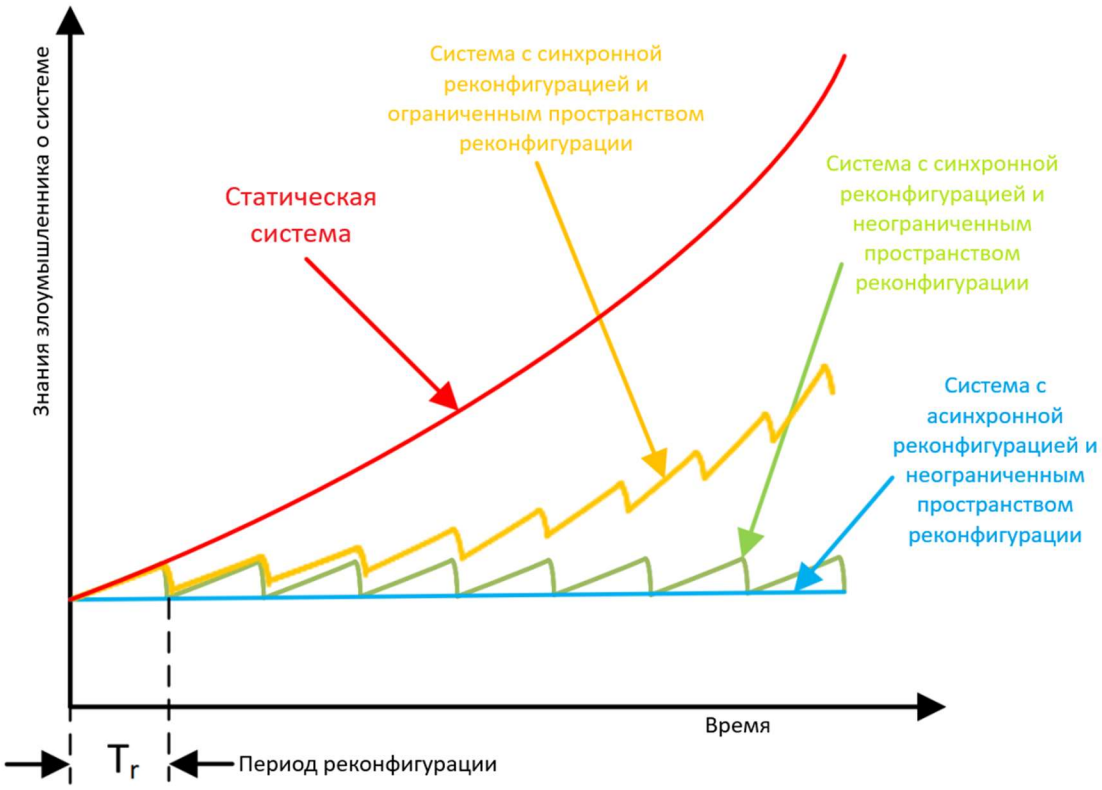

Рисунок 3 – График зависимости знаний злоумышленника о системе от времени

2.3 Оценка вероятности идентификации целевого хоста на основе математической модели

В качестве основы для математической модели взята математическая модель информационной сети на основе теории графов [133]. Основная её модификация заключается в изменении взаимосвязей между хостами в течение времени.

2.3.1 Математическая модель локальной сети передачи данных

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 хостами 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.

Внутри данной сети происходит постоянный процесс передачи сообщений: в соответствие с заданной частотой ν каждое устройство передает сообщение равновероятно по одному из маршрутов передачи сообщений, перечисленных в множестве W. Отправляемые сообщения содержат в себе ин-

формацию об отправителе и получателе, а также о следующем шлюзе. При этом допускается, что сообщения доставляются мгновенно и пропускной способностью каналов передачи информации можно пренебречь.

2.3.2 Модель злоумышленника при стратегии исследования при помощи сканирования

Данная модель подвергается атаке со стороны злоумышленника, включающей в себя две возможные глобальные стратегии [114].

Первая, наиболее простая, включает в себя активное сканирование всех возможных адресов в сети. В таком случае, если искомой целью злоумышленника является один конкретный хост v_i, а хосты в свою очередь распределены случайно по всем адресам сети, то ему придется придерживаться следующей стратегии.

Во-первых, прежде чем проводить попытку идентификации, злоумышленнику необходимо узнать, за какими адресами в сети находятся функционирующие устройства, для чего он будет проводить сканирование.

Во-вторых, сам процесс сканирования сети будет занимать время, оцениваемое по формуле (2):

$$t_{\text{ск.}} = N_{\text{адр}} \cdot t_{\text{ска.}}, \quad (2)$$

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

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

В-третьих, после завершения процесса сканирования злоумышленник получит список проверенных адресов сети мощностью N, после чего начнет процесс идентификации хостов. В процессе идентификации вероятность успешного опознания нужного хоста v_i будет составлять (3):

$$N_{\text{поп.}}/N, \quad (3)$$

где $N_{\text{поп.}}$– количество попыток идентификации со стороны злоумышленника.

Таким образом, наилучшей стратегией защиты в данном случае является определение критичного количества попыток идентификации $N_{\text{поп.кр.}}$ через

верхнюю границу вероятности обнаружения целевого хоста $p_{\text{кр.}}$ при помощи соотношения (4):

$$N_{\text{поп.кр.}} = N \cdot p_{\text{кр.}} \quad (4)$$

А задание периода реконфигурации топологии сетевого уровня равно (5):

$$\tau_{\text{р.}} = N_{\text{поп.кр.}} \cdot t_{\text{ид.}} + t_{\text{ск.}} = p_{\text{кр.}} \cdot N \cdot t_{\text{ид.}} + t_{\text{ск.}}, \quad (5)$$

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

При отсутствии введения такового среднее время идентификации целевого хоста будет составлять в среднем (6):

$$t_{\text{оп.}} = (N/2) \cdot t_{\text{ид.}} + N_{\text{адр}} \cdot t_{\text{ска.}} \quad (6)$$

В-четвертых, заметим, что злоумышленник может оптимизировать свою стратегию поиска с точки зрения скорости обнаружения целевого хоста, если будет производить попытку идентификации сразу после обнаружения очередного адреса, соответствующего устройству в сети. В таком случае среднее время на идентификацию хостов сети составит (7):

$$t_{\text{оп.опт.}} = 0.5\left(N \cdot t_{\text{ид.}} + N_{\text{адр}} \cdot t_{\text{ска.}}\right) \quad (7)$$

А период реконфигурации будет задаваться как (8):

$$\tau_{\text{р.}} = p_{\text{кр.}}\left(N \cdot t_{\text{ид.}} + N_{\text{адр}} \cdot t_{\text{ска.}}\right) \quad (8)$$

2.3.3 Модель злоумышленника при стратегии исследования при помощи пассивного перехвата и анализа

Вторая стратегия злоумышленника исходит из предположения, что сканирование сети вызовет срабатывание системы обнаружения и приведет к реконфигурации модели, поэтому злоумышленнику придется использовать стратегию внедрения в сеть и пассивного перехвата и анализа трафика с целью выявления адресов, по которым потенциально может располагаться целевой хост. В результате предполагаемая стратегия злоумышленника будет выглядеть следующим образом.

С точки зрения злоумышленника, исследуемая локальная сеть передачи данных представляет собой множество вершин $V_{\text{зл.}}$, соответствующее множеству адресов, известных ему и по которым распределены хосты – вершины графа G. Отметим, что поскольку модель реконфигурации каждый раз случайно распределяет хосты по адресам сети без учета информации о предыдущем распределении, то в начале каждой итерации реконфигурации $V_{\text{зл.}}$ будет соответствовать пустому множеству $\emptyset$. В процессе анализа сети для того, чтобы добавить адрес некоторой вершины v_i в множество $V_{\text{зл.}}$, злоумышленнику необходимо получить информацию о том, по какому адресу в сети располагается данный хост. Для этого злоумышленник в начале каждой итерации способен «внедриться» в некоторую случайную вершину $v_{\text{зр.}}$, после чего он будет способен перехватывать все сетевые пакеты, включенные в маршруты, проходящие через «зараженную» вершину. После сбора необходимой информации об адресах хостов в сети у злоумышленника будет лишь одна попытка идентификации необходимой ему вершины среди известных ему адресов, так как после этого события система обнаружения выявит злоумышленника, и он будет изолирован от сети.

Само множество вершин $V_{\text{зл.}}$ в конечном итоге представляет собой те вершины, для которых $v_{\text{зр.}}$ является элементом маршрута передачи информации (при этом неважно, конечным или промежуточным пунктом), и соответственно выражается через множество маршрутов W (9):

$$V_{\text{зл.}} = \{x \in w_i : v_{\text{зр.}} \in w_i, w_i \in W\} \tag{9}$$

Обозначим множество $V_{\text{зл.}}$ при выборе определенной вершины v_i в качестве зараженной вершины как $V_{\text{зл.}}(v_i)$. В таком случае, среднее количество известных злоумышленнику вершин $N_{\text{и}}$ будет равно (10):

$$N_{\text{и}} = \frac{1}{N} \sum_{v_i \in V} |V_{\text{зл.}}(v_i)| \tag{10}$$

Общая вероятность идентификации хостов сети при стратегии с пассивным перехватом и анализом складывается последовательно из двух событий:

1. Злоумышленник выбрал зараженную вершину таким образом, что через нее проходит канал общения целевой вершины с другими.

2. Злоумышленник смог из всего множества известных ему вершин выбрать ту, которая соответствует целевому хосту.

Поскольку зараженная и целевая вершина выбираются случайным образом, то вероятность первого события (11):

$$P_1 = N_и/N, \tag{11}$$

где $N_и$ – среднее число известных злоумышленнику вершин;

N – общее количество вершин в графе сети.

Поскольку злоумышленник лишь знает адреса сети, которым соответствуют хосты сети, но не распределение самих хостов, то выбирать из известных ему придется опять случайным образом и шанс второго события (12):

$$P_2 = 1/N_и \tag{12}$$

Таким образом, общая вероятность идентификации целевого хоста в сети при стратегии пассивного перехвата и анализа равна (13):

$$P_к = P_1 \cdot P_2 = \frac{N_и}{N} \cdot \frac{1}{N_и} = \frac{1}{N} \tag{13}$$

2.3.4 Ограничения математической модели

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 $t_{ска.}$ и $t_{ид.}$.

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.

2.3.5 Оценка периода реконфигурации

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 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 (14):

$$\rho(v_i) = 1 - \prod_{v_j \in V} \left(1 - \frac{\alpha(v_j, v_i)}{\beta(v_j)}\right), \tag{14}$$

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 $t_1, t_2, \dots, t_n$ – неубывающая последовательность, где t_i – среднее время ожидания, за который 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) [115]. Тогда получим следующий набор (15).

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 (прини-

мая $F_{N_и} = \tau_{кр.}$) произвести оценку критичного периода реконфигурации топологии сетевого уровня.

$$\begin{gathered} F_1 = t_1 + t_{обр.}, \\ F_2 = F_1 + ReLU(t_2 - F_1) + t_{обр.}, \\ \vdots \\ F_i = F_{i-1} + ReLU(t_i - F_{i-1}) + t_{обр.} \end{gathered} \quad (15)$$

2.3.6 Оценка результатов математического моделирования

Результаты математического моделирования показывают, что вероятность идентификации целевого хоста злоумышленником, как в случае сканирования, так и в случае пассивного перехвата и анализа трафика сети, на каждой итерации работы предложенного метода составляет $1/N$, где N – это количество хостов сети. Длительность актуальности текущей конфигурации топологии сетевого уровня, при которой вероятность идентификации целевого хоста злоумышленником остается равной $1/N$, вычисляется для каждой инфраструктуры индивидуально, и зависит она от следующих факторов: количество хостов сети и характер распределения трафика между хостами. Соответственно, данную величину можно корректировать путем добавления дополнительных ложных хостов в сеть, которые будут генерировать дополнительный ложный трафик.

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 [125]. 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.

2.4 Алгоритм формирования топологии сетевого уровня

Для того, чтобы оценить эффективность предложенного метода и подтвердить оценку вероятности при помощи математической модели на практике, необходимо реализовать предложенный метод. Для этого, необходимо разработать алгоритм формирования топологии сетевого уровня, а затем на основе метода и данного алгоритма разработать программное средство.

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 формирует одну новую работоспособную топологию из всех возможных топологий и сводит вероятность идентификации целевого хоста к $1/N$, где N – это количество хостов сети. Алгоритм формирования топологии сетевого уровня периодически заново используется для генерации новой топологии, тем самым обеспечивая её постоянную реконфигурацию.

Для одной из возможных реализаций алгоритма формирования топологии сетевого уровня введем несколько понятий, которые даны в словаре терминов: сеть MTD, физическое описание сети, участник взаимодействия, участник-сервер, участник-клиент, группа участников взаимодействия, внутренний и внешний участник-шлюз, потенциально опасный хост, правила исключения.

2.4.1 Реконфигурация топологии сетевого уровня

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 сканирование 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.

2.4.2 Формирование топологии сетевого уровня

Алгоритм формирования топологии сетевого уровня представлен на рисунке 4.

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 с MTD функционировала, должно быть, как минимум, два участника взаимодействия.

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 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.

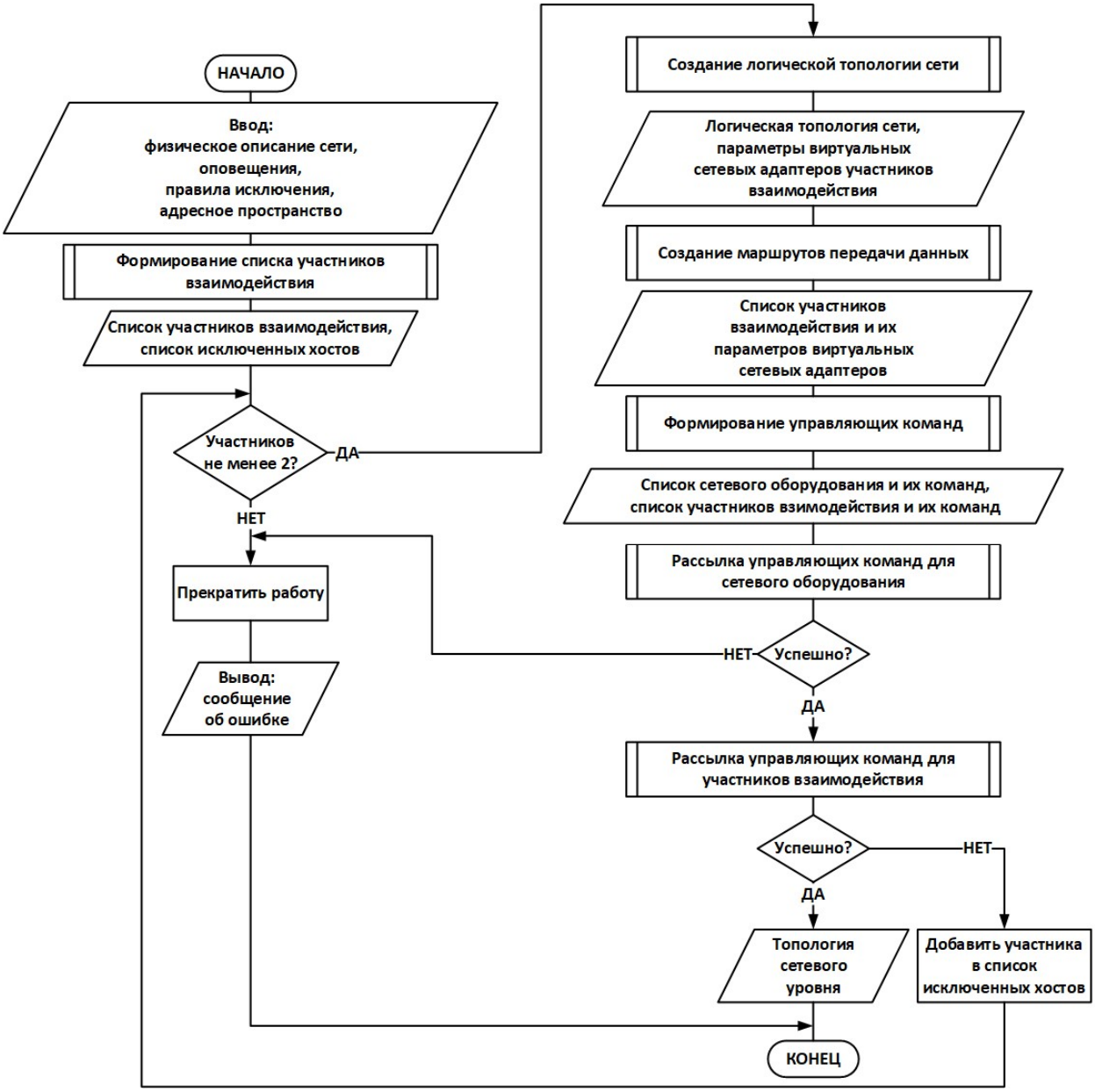

Рисунок 4 – Алгоритм формирования топологии сетевого уровня

2.4.3 Формирование списка участников взаимодействия

Первым шагом при формировании топологии сетевого уровня является формирование списков участников взаимодействия, алгоритм которого представлен на рисунке 5.

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.

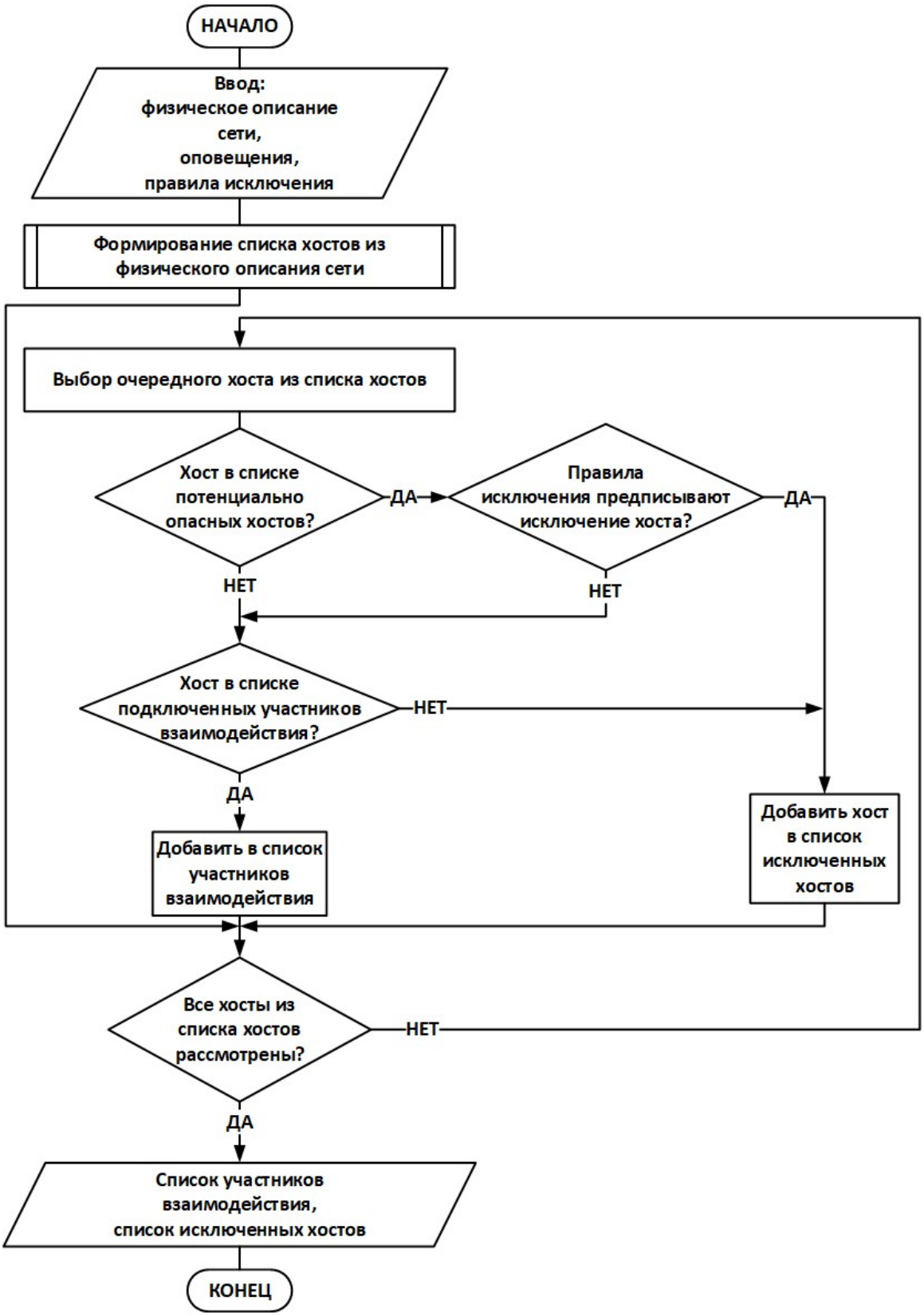

Рисунок 5 – Алгоритм создания списка участников взаимодействия

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.

Правила исключения определяются администратором сети MTD.

2.4.3 Создание логической топологии сети

Вторым шагом при формировании топологии сетевого уровня является создание логической топологии сети (рисунок 6). Логическая топология сети строится путем деления участников взаимодействия на группы.

Каждая группа образует выделенную подсеть. Внутри каждой группы один участник взаимодействия выбирается в качестве внутреннего 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.

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.

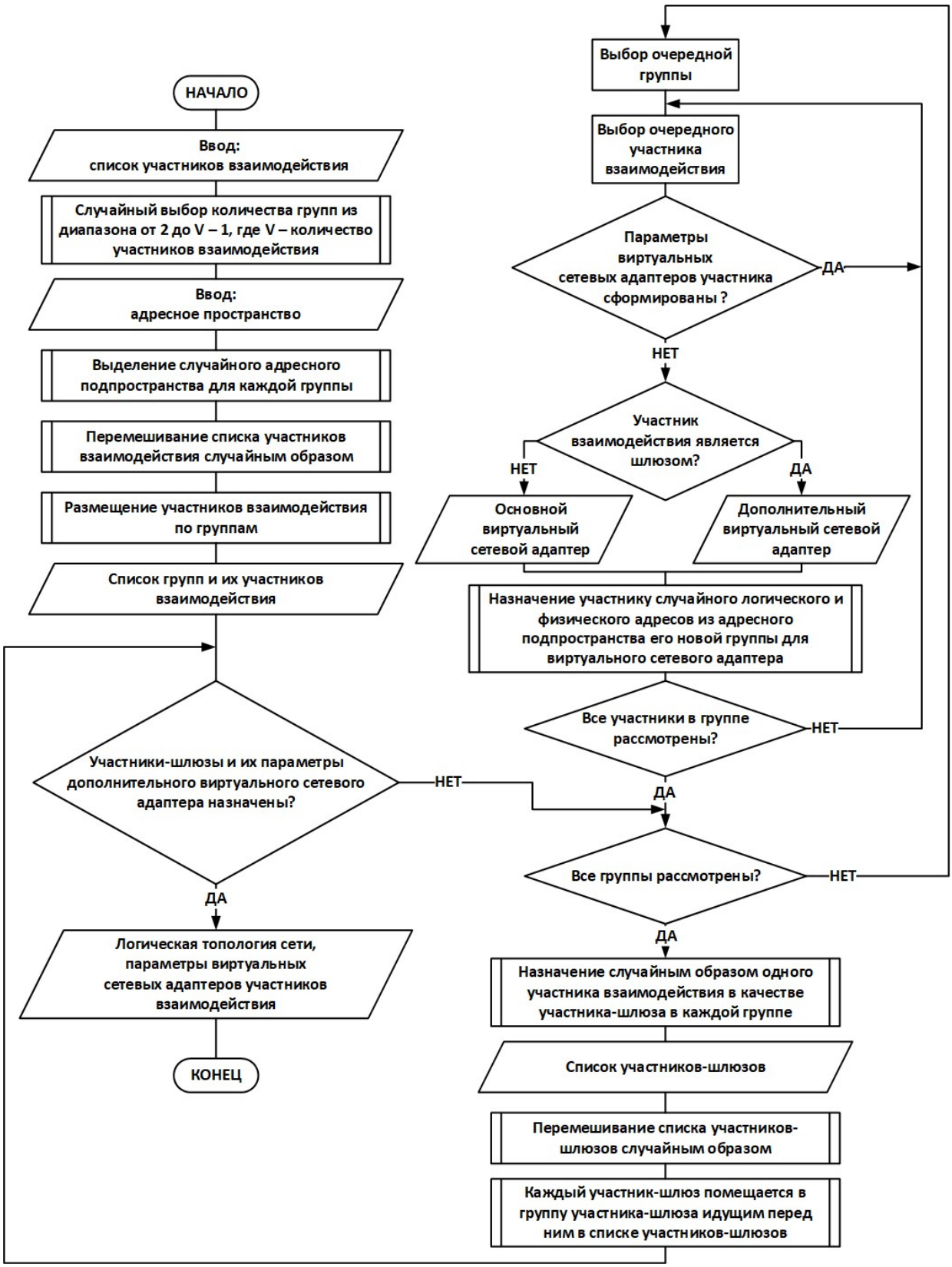

Рисунок 6 – Алгоритм создания логической топологии сети

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 $O(n)$.

2.4.4 Создание маршрутов передачи данных

Третьим шагом в формировании топологии сетевого уровня является построение маршрутов передачи данных (рисунок 7).

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.

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 $O(n^2)$.

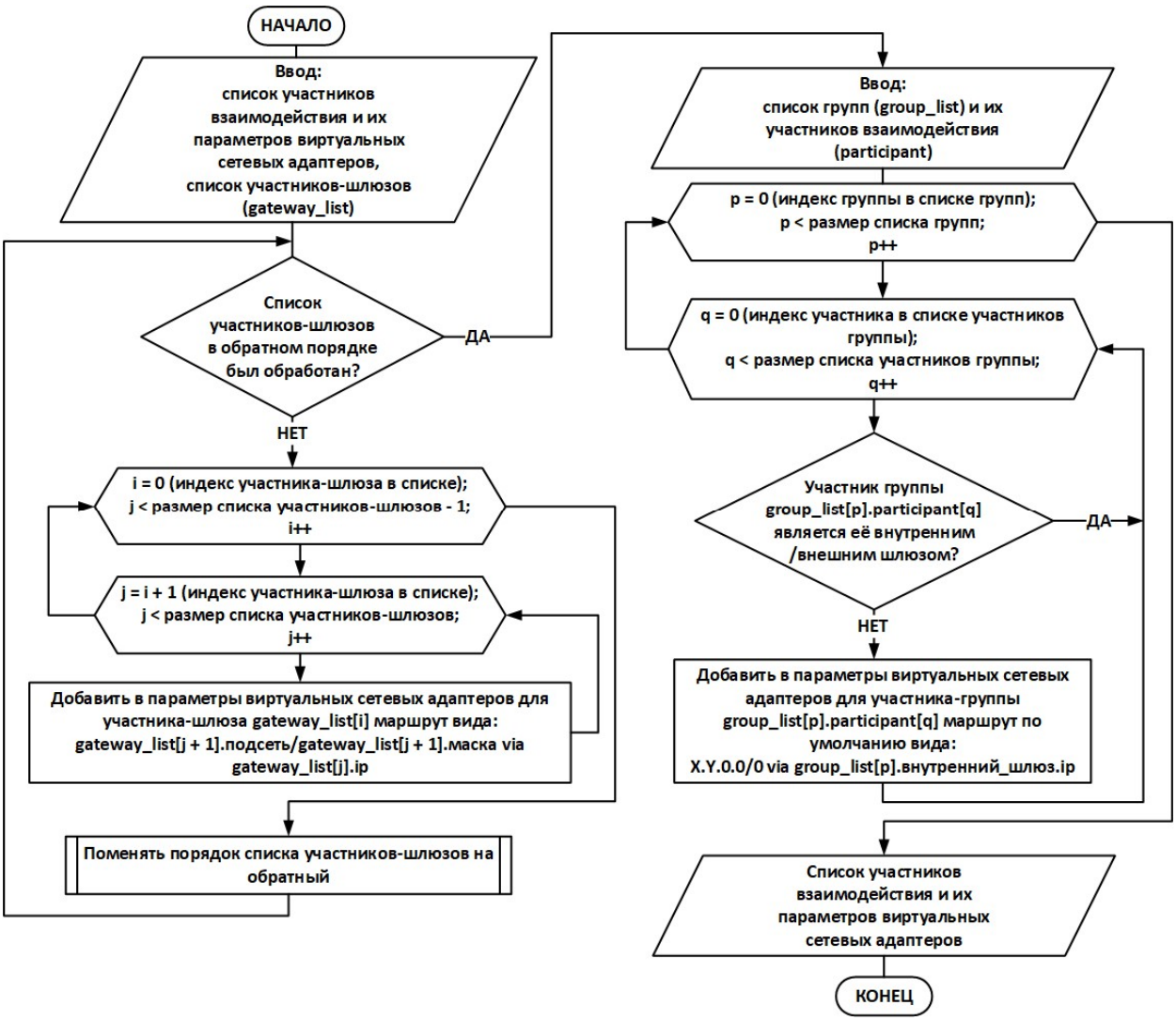

Рисунок 7 – Алгоритм построения маршрутов передачи данных

2.4.5 Создание управляющих команд

Четвертый шаг – создание управляющих команд (рисунок 8).

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.

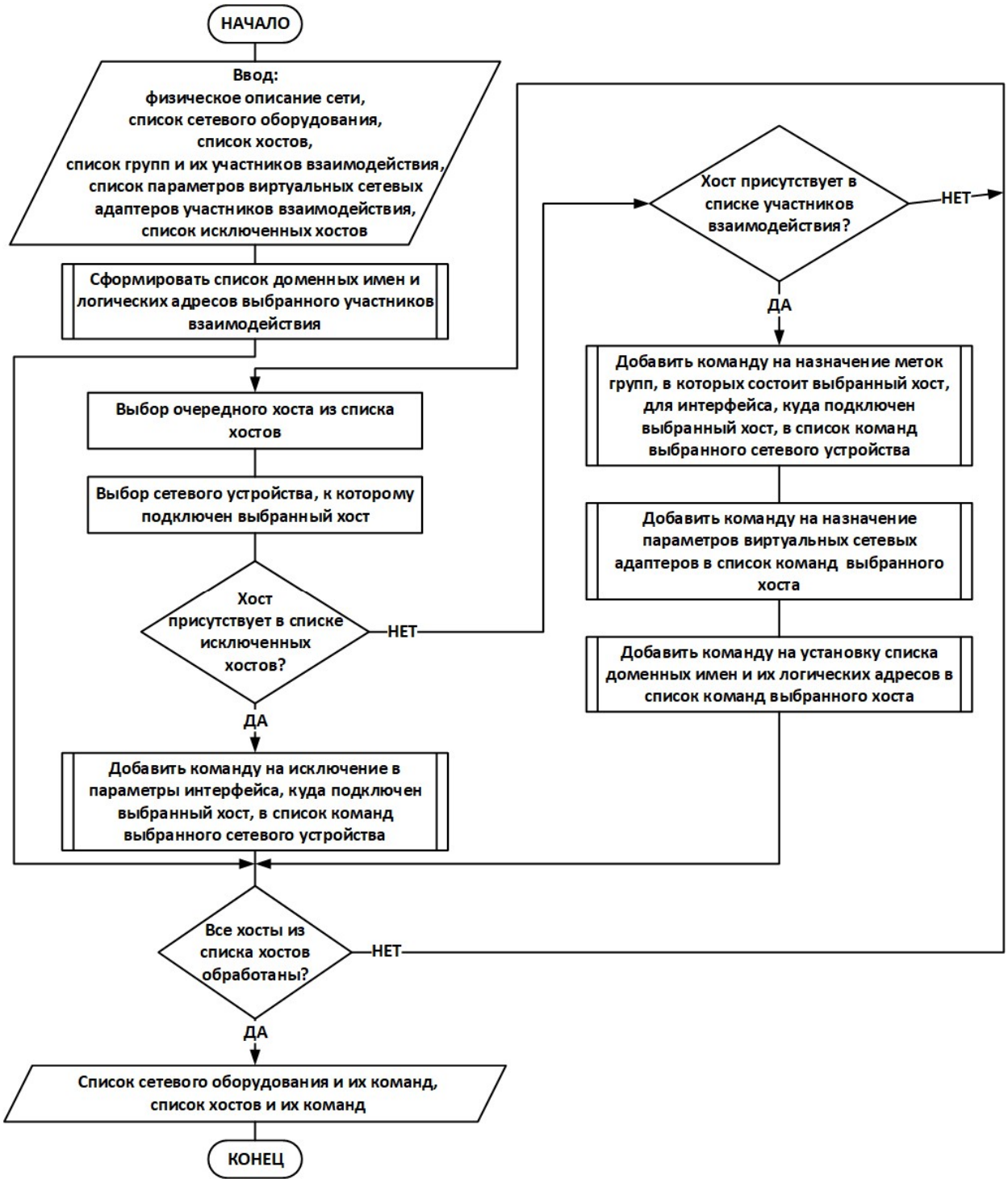

Рисунок 8 – Алгоритм создания управляющих команд

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.

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

2.4.6 Рассылка управляющих команд

Пятый шаг – рассылка управляющих команд. 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 по сети через API, 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. На рисунке 9 приведена схема-пример простой физической инфраструктуры.

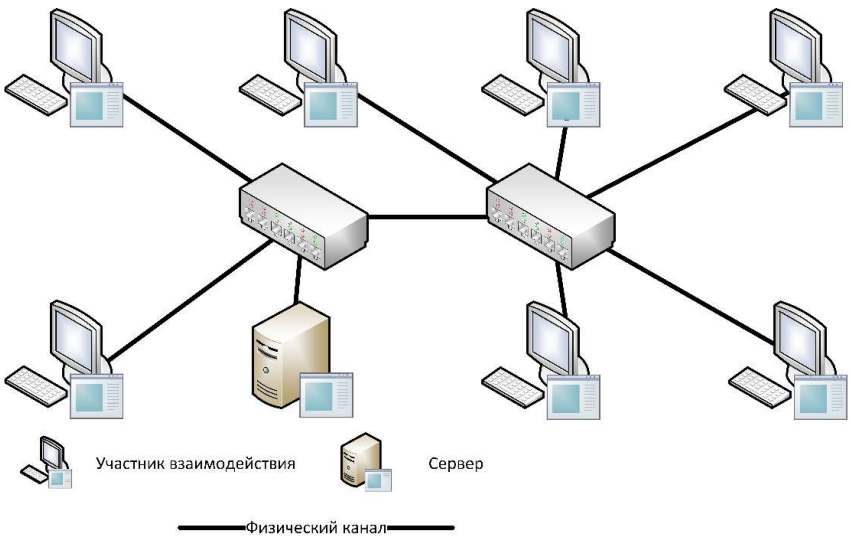

Рисунок 9 – Схема простой физической инфраструктуры

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 хосты-участники не сообщили об успешном приеме конфигурации, они исключаются из списка подключенных, а топология сетевого уровня реконфигурируется заново.

2.4.7 Действие предложенного метода и алгоритма

Результирующая сложность алгоритма формирования топологии сетевого уровня составляет $O(n) + O(n) + O(n^2) + O(n)$, что равно $O(n^2)$.

Действие предложенного метода и алгоритма можно представить в виде схем. Хосты сети MTD были распределены на группы (рисунок 10). А затем были построены маршруты передачи данных (рисунок 11). Значения адресов и подсетей упрощены для понимания принципов построения маршрутов. По истечению временного периода произошла реконфигурация топологии сети (рисунок 12), то есть была создана новая работоспособная топология сетевого уровня, и старая топология была заменена ею (рисунок 13). После чего, в результате обнаружения потенциально опасного хоста, была сформирована еще одна новая топология сетевого уровня, из которой он был исключен.

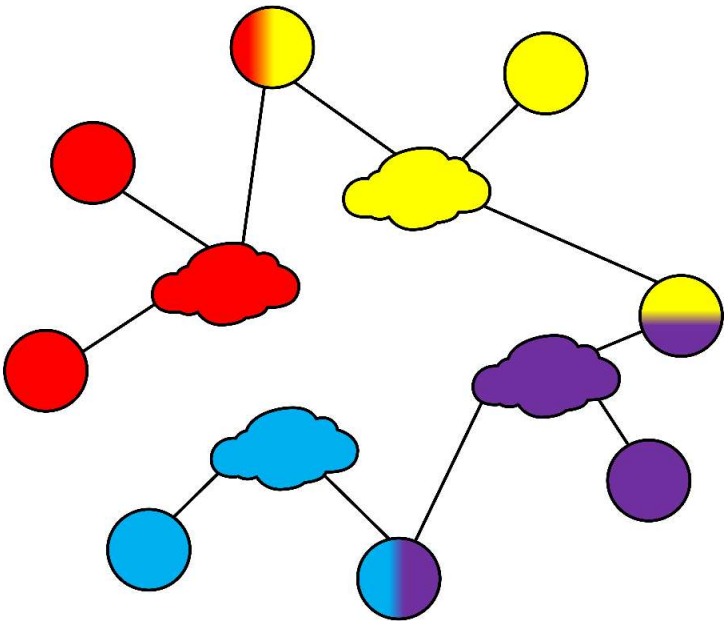

Рисунок 10 – Распределение узлов на группы и их соединение

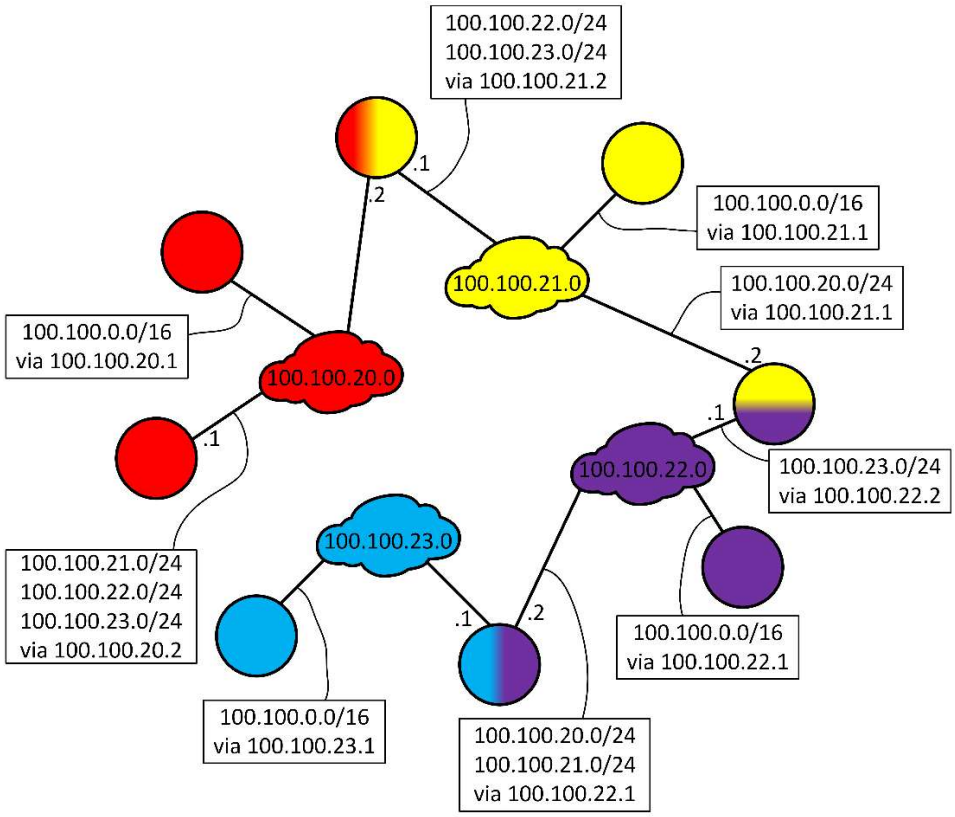

Рисунок 11 – Построение маршрутов передачи данных

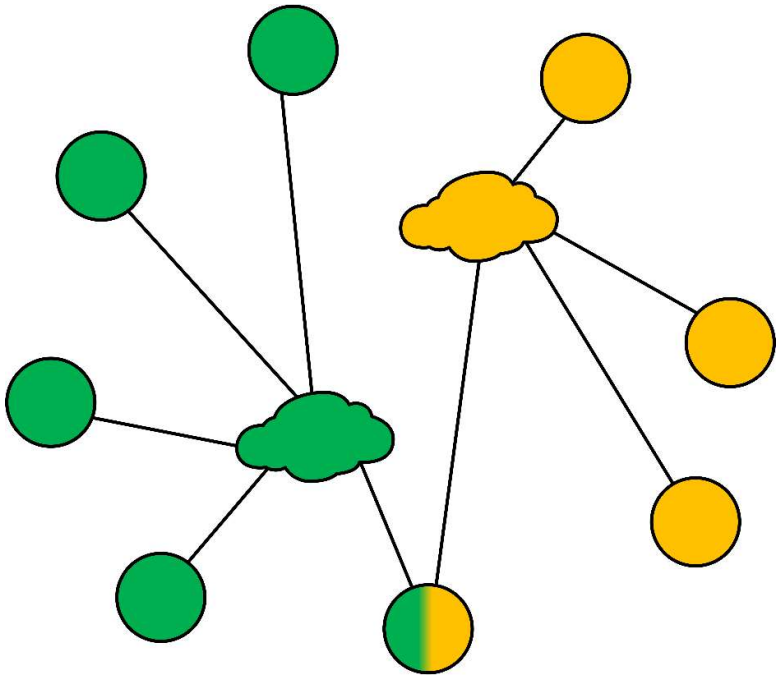

Рисунок 12 – Создание новой топологии сетевого уровня в результате истечения временного периода

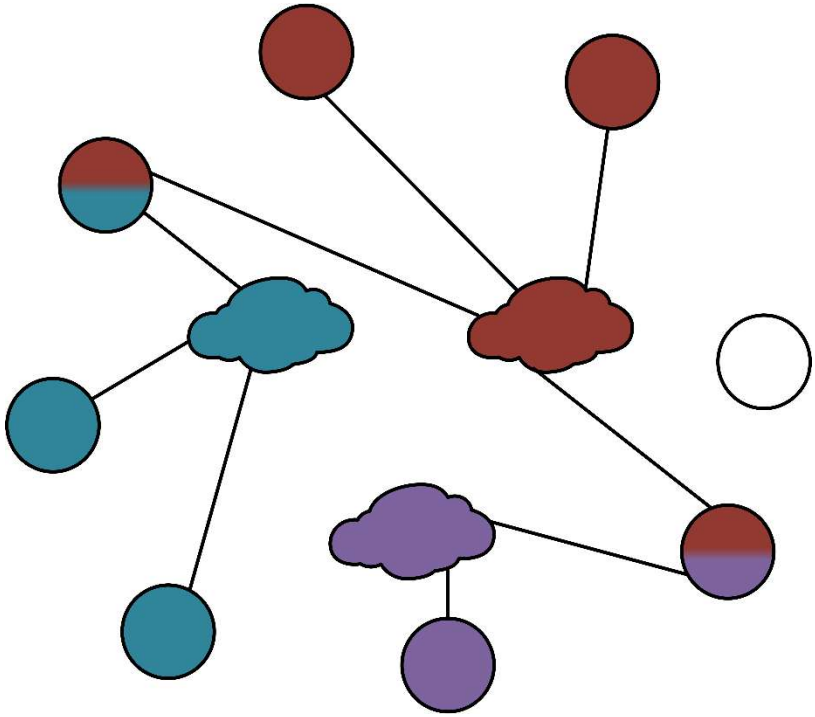

Рисунок 13 – Создание новой топологии сетевого уровня в результате обнаружения потенциально опасного узла

Такие постоянные реконфигурации топологии сетевого уровня должны привести к тому, чтобы злоумышленник не мог обладать долговременной полезной информацией об организации локальной сети передачи данных, так как хосты при каждой новой итерации метода имеют новые адреса, как физические, так и логические, а маршруты передачи данных и логическая топология также изменяются.

2.4.8 Противодействие потенциальным угрозам

Далее необходимо определить, как именно алгоритмическая реализация предложенного метода противостоит потенциальным угрозам.

1. Угроза обнаружения узлов и угроза определения топологии вычислительной сети.

Ключевым элементом обнаружения узлов и определения топологии является возможность идентификации хостов и сопоставления их адресов в сети. Предложенная реализация и метод в целом противостоят этой угрозе, динамически изменяя 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.

В сканировании сети злоумышленник никак не ограничен до тех пор, пока не будет обнаружен. В случае обнаружения он может быть изолирован. Дополнительно можно усилить метод при помощи динамического создания новых ложных хостов, таким образом изменяя количество хостов сети MTD. В результате у злоумышленника будет создано ложное представление о реальном составе сети. Однако такое усиление остается за рамками настоящей работы.

2. Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб, а также угроза определения типов объектов защиты.

Так как предложенный метод не манипулирует ПО, расположенным на хостах, открытые порты и привязанные к ним службы остаются статичными. Собранная злоумышленником информация о хостах в период между реконфигурациями может быть актуальной и полезной, так как по набору открытых портов могут выделяться отдельные хосты из общей массы, и они в последствии могут быть легко идентифицированы независимо от смены адресов, маршрутов передачи и логической топологии. Для решения данной проблемы необходимо сконфигурировать ПО, расположенное на хостах, таким образом, чтобы хосты не отличались друг от друга по набору портов. Даже если необходимости в этих службах на узле нет, все равно следует создать ложное впечатление об их наличии. Таким образом, сеть MTD будет выглядеть для злоумышленника как сеть идентичных хостов с постоянным изменением топологии сетевого уровня.

В сканировании портов и определении типов объектов защиты злоумышленник никак не ограничен до тех пор, пока не будет обнаружен. В случае обнаружения он может быть изолирован. Дополнительно можно усилить

предложенный метод динамической реконфигурацией ПО, расположенного на каждом хосте, чтобы у злоумышленника создалось ложное впечатление о том, что на каждой итерации создаются совершенно новые хосты, а старые исчезают. Однако такое усиление остается за рамками настоящей работы.

3. Угроза перехвата данных, передаваемых по вычислительной сети.

Предложенный метод противостоит этой угрозе, так как собранная информация о сети перестает быть актуальной после реконфигурации. В перехвате данных злоумышленник никак не ограничен до тех пор, пока не будет обнаружен. В случае, если конфиденциальная информация передается по сети в открытом виде, злоумышленник может её перехватить и извлечь. Для усиления предложенного метода необходимо передавать информацию только в зашифрованном виде.

4. Угроза получения предварительной информации об объекте защиты. Предположим, что в сети MTD функционирует реальная сетевая служба, которая имеет критическую уязвимость. В случае, если ПО, расположенное на хостах, сконфигурировано таким образом, чтобы состав открытых портов каждого хоста не отличались друг от друга, то для злоумышленника каждый хост будет обладать такой службой и такой уязвимостью, хотя в реальности служба является фиктивной. Как следствие, даже если злоумышленник за период до реконфигурации установит хост с реальной службой, то на следующей реконфигурации он будет вынужден искать его заново.

Как итог, метод может противодействовать всем актуальным угрозам, связанным со сторонним исследованием локальной сети передачи данных.

2.5 Программная реализация предложенного метода

Для того, чтобы провести эмпирическую оценку предложенных метода и алгоритма, необходимо разработать их программную реализацию. Это способствует прозрачности, воспроизводимости и повторяемости исследования. Программная реализация также необходима для прямого решения проблемы защиты локальной сети передачи данных от исследования злоумышленником.

2.5.1 Выбор технологий для реализации метода и алгоритма

По своей сути в основе предложенного алгоритма лежит SDN, поэтому в качестве базовой технологии, в рамках которой будет осуществляться реконфигурация топологии сетевого уровня, выбрана технология Virtual eXtensible Local Area Network (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.

VXLAN – это технология оверлея, которая инкапсулирует кадры Ethernet 2-го уровня в пакеты User Datagram Protocol (UDP) 3-го уровня, позволяя распространять сегменты 2-го уровня в сетях 3-го уровня. Инкапсуляция добавляет дополнительный заголовок к исходному кадру Ethernet, который включает 24-битный идентификатор сети VXLAN (VNI), значительно расширяя количество доступных сегментов сети.

SDN характеризуется отделением плоскости управления от плоскости данных, что позволяет осуществлять централизованное управление и динамическую конфигурацию сети. VXLAN вносит свой вклад в эту парадигму, абстрагируя базовую физическую сеть, позволяя создавать виртуальные сети, которыми можно программно управлять. Оверлейный характер VXLAN позволяет контроллерам SDN реализовывать виртуальные топологии независимо от физической инфраструктуры, способствуя быстрому развертыванию сервисов и приложений. Интегрируя VXLAN с контроллерами SDN, системные администраторы могут получить централизованный контроль над виртуальной сетевой средой. VXLAN позволяет сократить ненужный широковещательный трафик за счет использования эффективных методов репликации, повышая общую эффективность сети по сравнению с традиционными широковещательными доменами VLAN. VLAN ограничены 4096 уникальными идентификаторами из-за 12-битного поля VLAN ID, определенного в стандарте IEEE 802.1Q. В отличие от него, в VXLAN используется 24-битный идентификатор сети VXLAN (VNI), что позволяет создавать до 16777216

уникальных сегментов сети. Также технология VXLAN позволяет создавать и изменять виртуальные сегменты сети «на лету». Эта ключевая особенность, которая позволяет MTD при помощи VXLAN эффективно решать задачи по защите локальной сети передачи данных от исследования злоумышленником [108].

Помимо того, что сетевое оборудование, на котором функционирует сеть MTD, должно поддерживать технологию VXLAN, также необходимо, чтобы оно могло управляться при помощи программ. То есть, сетевое оборудование должно предоставлять некоторый API, при помощи которого можно было бы осуществлять конфигурирование оборудования. Среди представленных на текущий момент решений, было выбрано решение от Cisco, поддерживающее технологию VXLAN и функционирующее под управлением ОС NX-OS. Данная ОС предоставляет NX-API, при помощи которого можно управлять сетевым устройством. Выбор был обусловлен не только возможностями по программному управлению и наличием API, но и более широкими возможностями в сравнении с другими решениями по созданию виртуальных стендов для исследований [109].

Взаимодействие с сетевым оборудованием построено на основе протокола JSON RPC 2.0 [110] через протокол HTTP. В ОС NX-OS развернут HTTP-сервер, который принимает POST-запросы, где в тело запроса вложен JSON-объект в формате спецификации JSON RPC 2.0. Взаимодействие с узлами было построено на основе протокола JSON RPC 2.0 через протокол WebSocket. Выбор WebSocket в качестве протокола связи обусловлен наличием расширенных возможностей по двунаправленной передаче данных, в отличие от HTTP [111].

Для хостов в качестве ОС была выбрана ОС семейства Linux, а именно Ubuntu 22.04. Её надежные функции, широкая поддержка сообщества и совместимость с различными инструментами SDN делают её хорошим выбором для реализации подобных решений. В частности, данная ОС поддерживает утилиту Netplan, которая предоставляет упрощенный согласованный способ

управления сложными сетевыми настройками с помощью человекочитаемых файлов формата YAML. Netplan поддерживает такие расширенные сетевые функции, например, как агрегация каналов, мосты, VLAN и IP-туннели, при этом позволяет подробно описать политики маршрутизации и настройки DNS [112].

В качестве системы для обнаружения исследования злоумышленником локальной сети передачи данных была выбрана СОВ Snort. Так как настоящая работа не рассматривает вопросы эффективного обнаружения злоумышленника в процессе исследования сети, выбор СОВ не является принципиальным.

В качестве языка программирования для реализации предложенного метода был выбран язык C++17 и фреймворк Qt 5.15, так как данный набор инструментов имеет в себе все необходимые библиотеки для быстрой разработки сетевых графических приложений. В качестве СУБД для хранения физического описания сети выбрана система SQLite, так как она проста, легковесна и не имеет доступа в сеть, но взаимодействие с БД предполагается осуществлять локально в рамках одного хоста. Таким образом технологический стек предложенного метода можно представить схемой, как на рисунке 14.

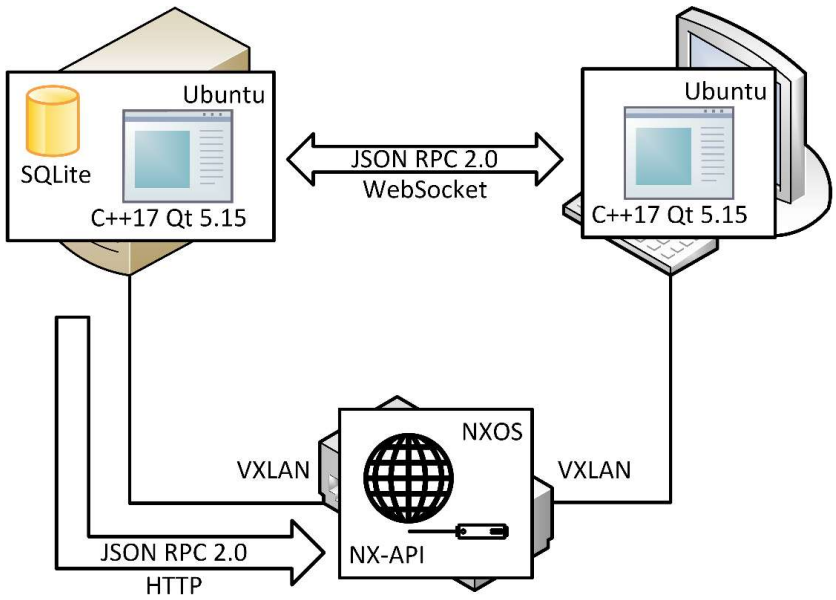

Рисунок 14 – Схема технологического стека предложенного метода

2.5.2 Описание общего взаимодействия

Описание взаимодействия между клиентом, сервером и сетевым оборудованием представлено на рисунке 15.

Для организации сети MTD передаются следующие данные: параметры виртуальных сетевых адаптеров хостов, списки доменных имен и соответствующих им адресов, списки потенциально опасных хостов, а также управляющие команды для сетевого оборудования.

На каждом хосте сети MTD запускается клиентская часть ПО, а на одном из них – и серверная часть ПО. Передаваемые данные упакованы в JSON-объекты в соответствии со спецификацией JSON RPC 2.0.

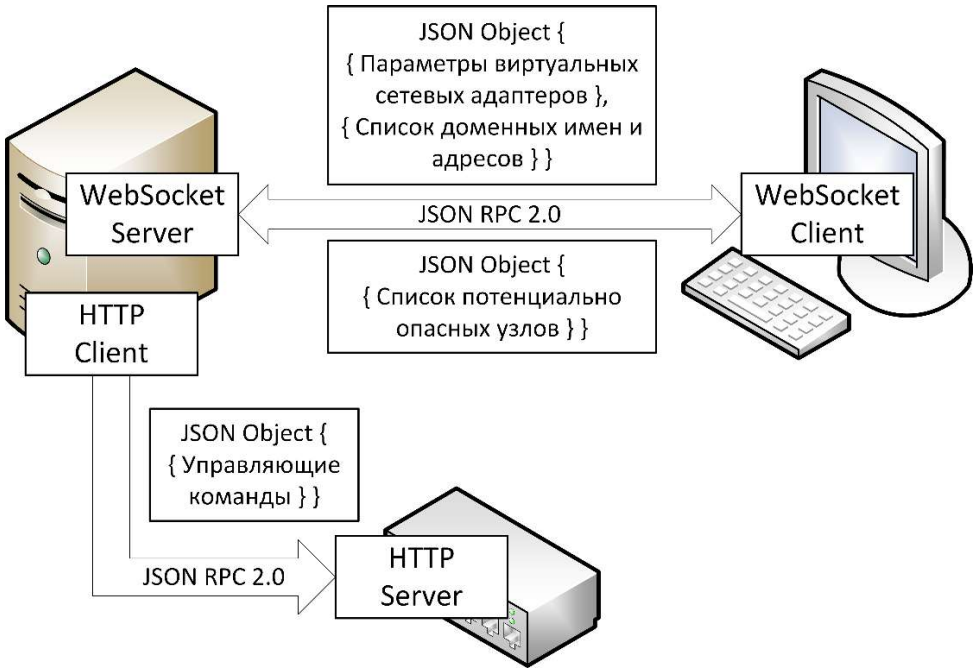

Рисунок 15 – Общая схема взаимодействия

2.5.3 Клиентская часть программного обеспечения

Схема клиентской части ПО представлена на рисунке 16.

Клиентская часть ПО принимает и обрабатывает JSON-объекты, которые содержат параметры виртуальных сетевых адаптеров, списки доменных имен и соответствующих им адресов. После извлечения этих параметров, клиентская часть ПО формирует требуемые конфигурационные файлы на их основе и инициирует реконфигурацию хоста.

В тоже время в фоновом режиме функционирует СОВ Snort, которая детектирует исследование сети злоумышленником. Клиентская часть ПО отслеживает специальный файл с предупреждениями СОВ Snort. В случае появления новой записи, клиентская часть ПО анализирует её и извлекает из неё адрес хоста, который необходимо изолировать. Таким образом формируется список потенциально опасных хостов, который передается участнику-серверу.

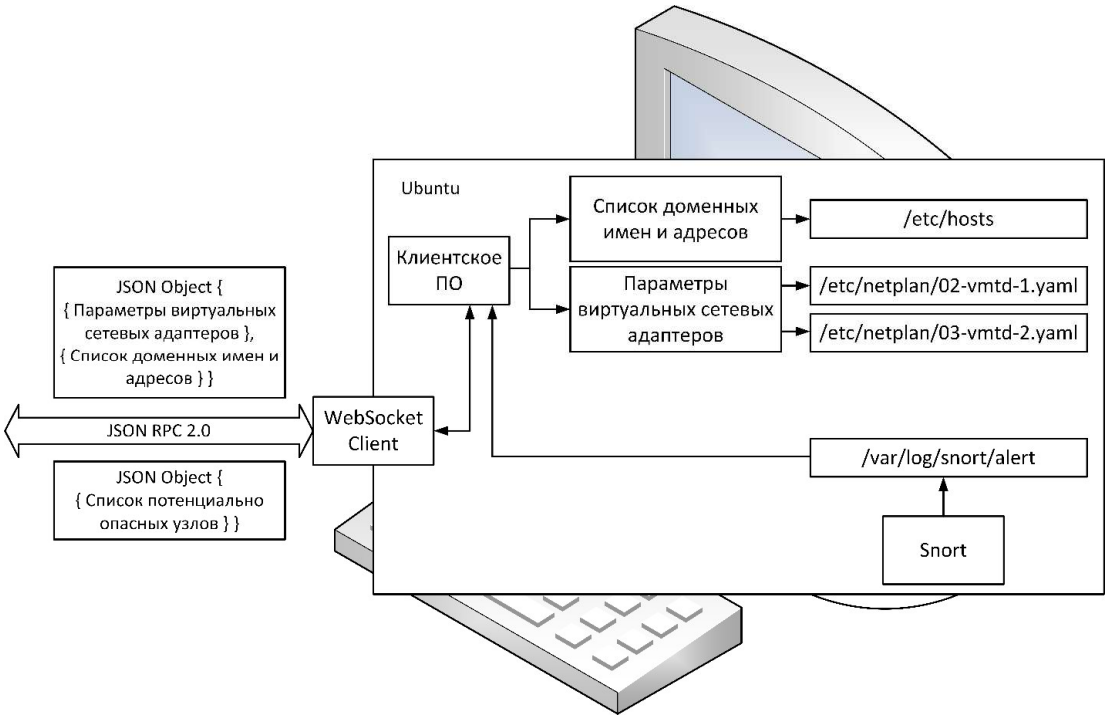

Рисунок 16 – Схема клиентской части ПО

С точки зрения организации программного кода, клиентская часть ПО состоит из следующих функциональных объектов:

1. Модуль, реализующий функционал WebSocket-клиента.

2. Модуль, реализующий обработку данных в соответствии со спецификацией JSON RPC 2.0 и соглашениями внутреннего протокола предложенного метода.

3. Модуль, осуществляющий ввод параметров виртуальных сетевых адаптеров и списка доменных имен и соответствующих им адресов.

4. Модуль, отслеживающий оповещения от СОВ.

2.5.4 Серверная часть программного обеспечения

Серверная часть ПО на основе физического описания сети, списка подключенных хостов и списка потенциально опасных хостов формирует параметры виртуальных сетевых адаптеров и управляющие команды для сетевого оборудования. После чего упаковывает параметры в JSON-объекты в соответствии со спецификацией JSON RPC 2.0 и отправляет через сеть по протоколу WebSocket для участников-клиентов, а для сетевого оборудования упаковывает команды в соответствии со спецификациями JSON RPC 2.0 и NX-API и отправляет по протоколу HTTP. База данных, содержащая физическое описание, приведена на рисунке 17.

Реконфигурация инициируется через заданные периоды времени или по появлению новых записей в списке потенциально опасных хостов. Физическое описание сети содержит список разрешенных сканирующих хостов, которые не изолируются по обнаружению их действий по исследованию сети.

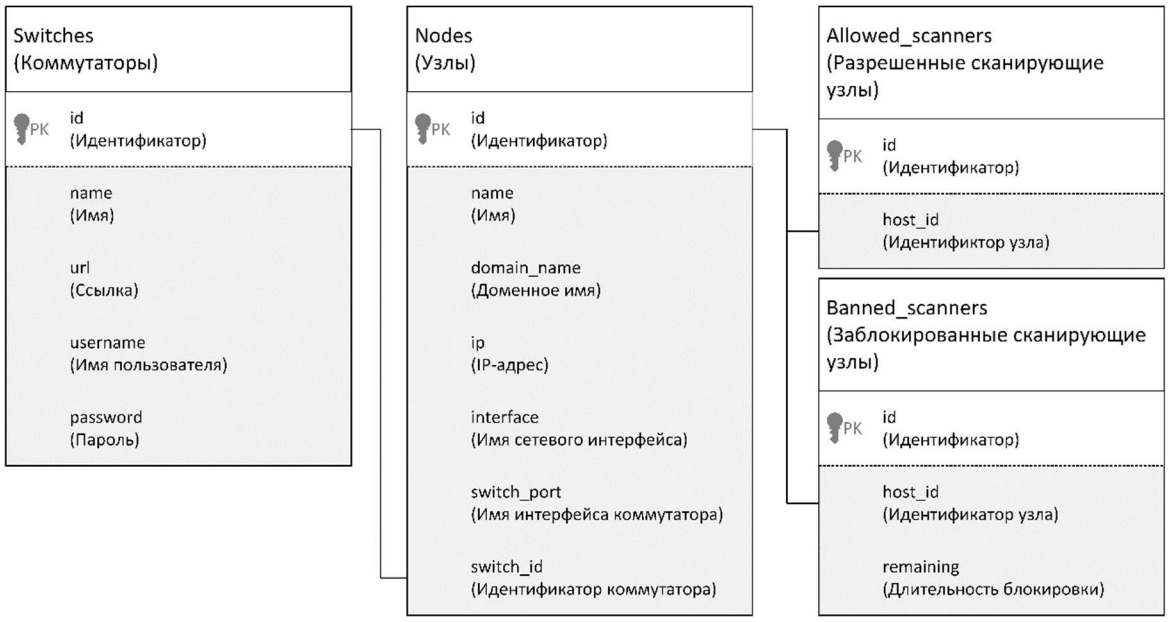

Рисунок 17 – Схема БД физического описания сети

Схема серверной части ПО представлена на рисунке 18.

С точки зрения организации программного кода, серверная часть ПО состоит из следующих функциональных объектов:

1. Модуль, реализующий функционал WebSocket-сервера.

2. Модуль, реализующий функционал HTTP-клиента.

3. Модуль, реализующий обработку данных в соответствии со спецификациями JSON RPC 2.0 и внутреннего протокола предложенного метода.

4. Модуль, реализующий обработку данных в соответствии со спецификациями JSON RPC 2.0 и NX-API.

5. Модуль, который отслеживает события (истечение временного периода или новые записи в списке потенциально опасных хостов), а также формирует и инициирует передачу новых параметров виртуальных сетевых адаптеров, список доменных имен и соответствующих им адресов для каждого участника-клиента, а также управляющие команды для сетевого оборудования.

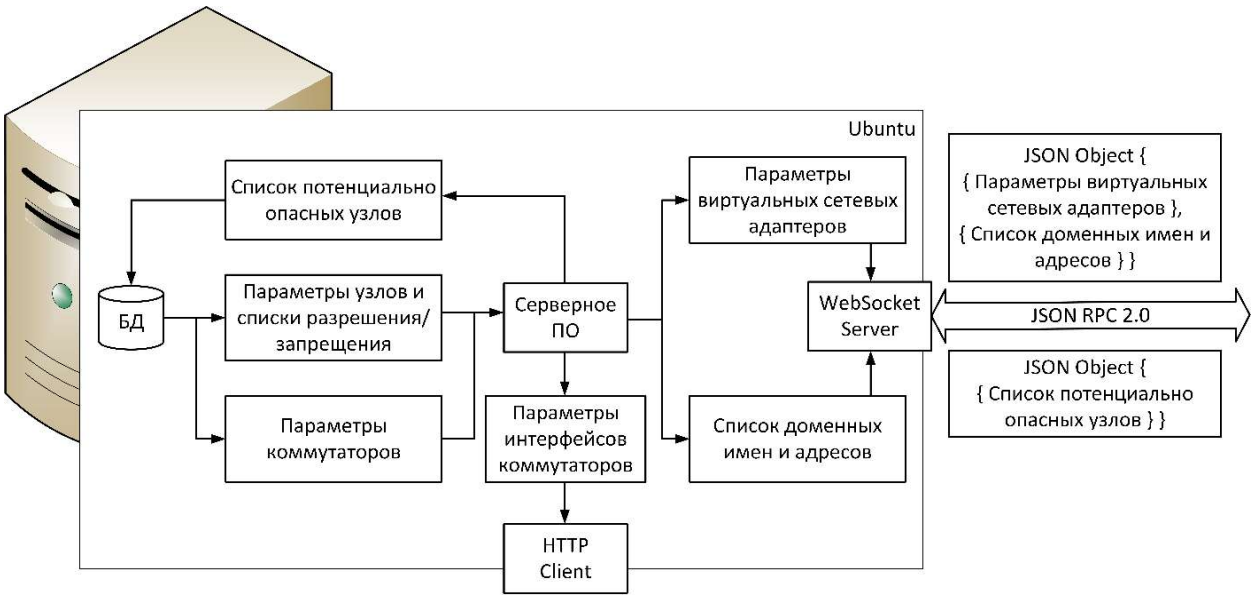

Рисунок 18 – Схема серверной части ПО

2.5.5 Формат конфигураций

Предложенный метод формирует список меток групп для интерфейсов сетевого оборудования, трафику которых позволено проходить через данный интерфейс. Это происходит по шаблону, представленному в таблице 3.

При рассмотрении шаблона может возникнуть вопрос о том, что в нем фигурирует VLAN ID, а не VNI, использование которого предполагает техно-

логия VXLAN. Все дело в том, что хосты не имеют сведений о том, при помощи какой технологии построено взаимодействие: VLAN или VXLAN. Для хостов нету разницы какая из этих технологий используется, они лишь помечают свой трафик определенным тегом, который показывает принадлежность к определенной виртуальной сети. Сетевое оборудование, при правильном конфигурировании VXLAN, уже внутри себя преобразует полученные VLAN ID в нужные VNI.

Таблица 3 – Шаблоны конфигурирования

Шаблон конфигурирования виртуального сетевого адаптера	Шаблон конфигурирования сетевого оборудования

network:
  vlans:
  vlan.<метка группы>:
  id: <метка группы>
  link: <имя сетевого адаптера>
  addresses: ["<ip-адрес/маска>"]
  macaddress: <mac-адрес>
  routes:
  - to: <целевая сеть/маска>
  via: <ip-адрес шлюза>
  metric: <метрика>
	interface <имя интерфейса>
	  switchport
	  switchport mode trunk
	  switchport trunk allowed vlan <метки групп>
	  no shutdown

Предложенный метод формирует следующие параметры виртуальных сетевых адаптеров: физический и логический адреса, маршруты передачи, метка группы. Эти параметры задаются при помощи предопределенного шаблона в специфичном для утилиты Netplan формате, который представлен в таблице 3.

Отдельно стоит отметить, как формируется участником-сервером IP-адрес и MAC-адрес. IP-адрес формируется следующим образом: 1-2 октет – фиксирован и задается администратором; 3 октет – выбирается случайным образом и соответствует метке группы; 4 октет – выбирается случайным образом. MAC-адрес формируется следующим образом: 1-4 октет – фиксирован и задается администратором, для того чтобы избежать конфликта физических

адресов; 5 октет – выбирается случайным образом и соответствует метке группы; 6 октет – выбирается случайным образом.

2.5.6 Протоколы взаимодействия

Форматы JSON-объектов, предназначенных для взаимодействия с сетевым оборудованием, приведены в приложении 1.

При взаимодействии с сетевым оборудованием в соответствии со спецификацией NX-API формируется JSON-объект и отправляется в сеть. В поле cmd указывается команда, которую необходимо выполнить. То есть для того, чтобы отправить весь шаблон, необходимо сформировать пять JSON-объектов, которые соответствуют строкам шаблона.

В свою очередь HTTP-сервер ответит: в случае правильной команды – HTTP-ответ в теле, которого будет JSON-объект, содержащий данные о завершении команды, а в случае неправильной команды – HTTP-ответ с кодом ошибки 400 Bad Request.

При взаимодействии с участниками взаимодействия формируется JSON-объект, в соответствии с внутренним протоколом. Протокол предполагает набор из 6 типов запросов в соответствии с приложением 2:

1. Установка параметров виртуального сетевого адаптера.

2. Очистка параметров виртуального сетевого адаптера.

3. Установка списка доменных имен и соответствующих им адресов.

4. Ввод установленных параметров виртуальных сетевых адаптеров и списка доменных имен и соответствующих им адресов.

5. Проверка наличия соединения.

6. Получить список потенциально опасных хостов.

Протокол взаимодействия с хостами сети MTD предполагает 6 типов ошибок:

1. -32700 Ошибка парсинга запроса. Ошибка формируется в том случае, когда из JSON-объекта невозможно извлечь данные.

2. -32600 Неверный запрос. Ошибка формируется в том случае, когда запрос не содержит в себе обязательные поля: *id, jsonrpc, method, params*.

3. -32601 Метод не найден. Поле *method* содержит то значение, которое не предусматривается протоколом взаимодействия.

4. -32602 Неверные параметры. Поле *params* не содержит в себе полей, которые необходимы для выполнения метода, либо значения этих полей некорректны.

5. -32603 Внутренняя ошибка. Используется в том случае, когда возникшая ошибка не соответствует ни одному из вышеуказанных типов ошибок.

2.5.7 Дополнительный функционал программного обеспечения

Программное обеспечение [113] реализует не только базовый функционал предложенного метода, но и некоторые дополнительные функции для удобства исследования и тестирования.

На рисунке 19-21 приведены основные окна ПО предложенного метода.

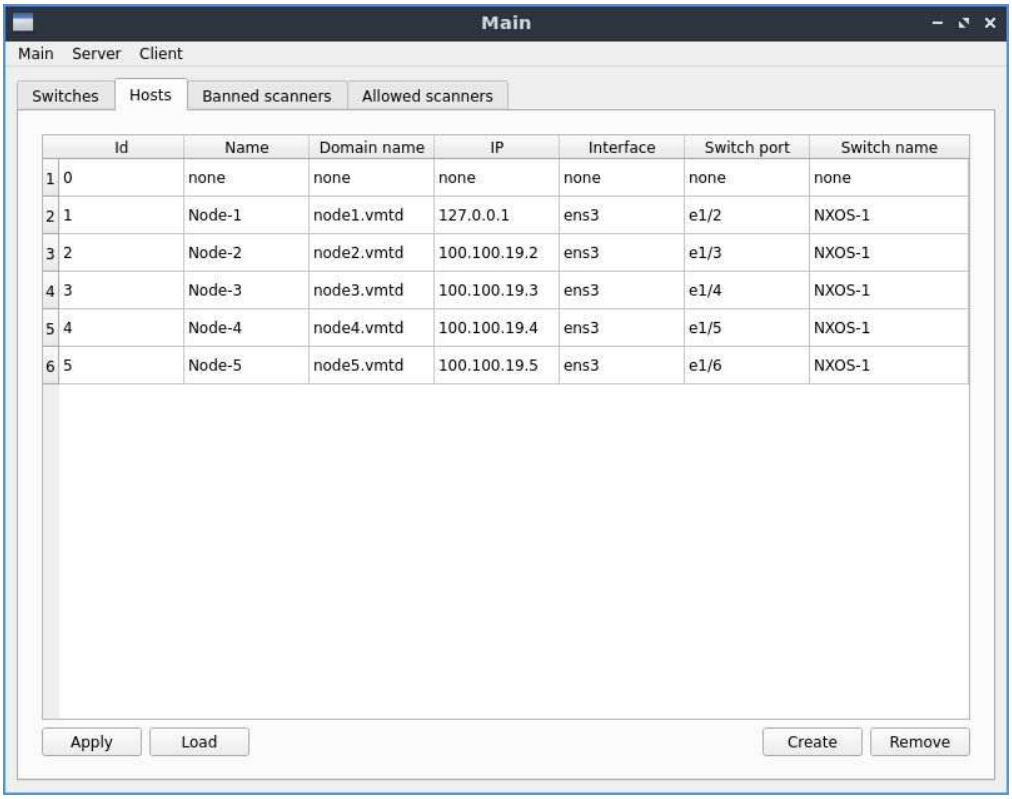

Рисунок 19 – Вкладка редактирования базы данных физического описания сети MTD

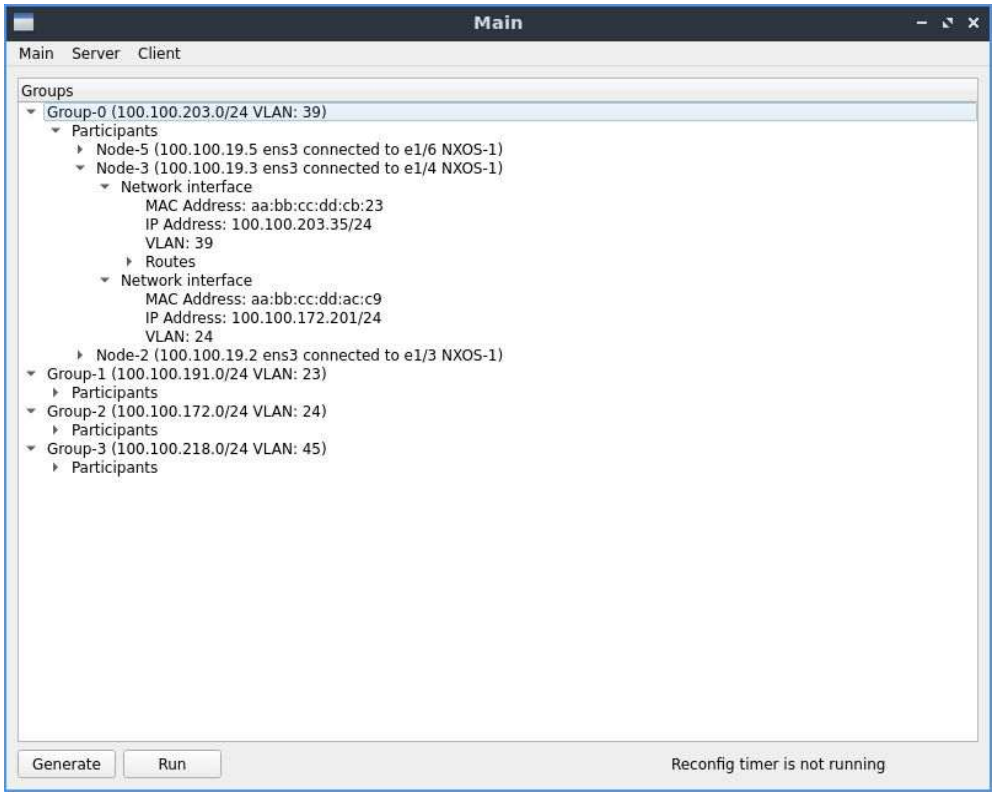

Рисунок 20 – Вкладка текущей конфигурации сети MTD

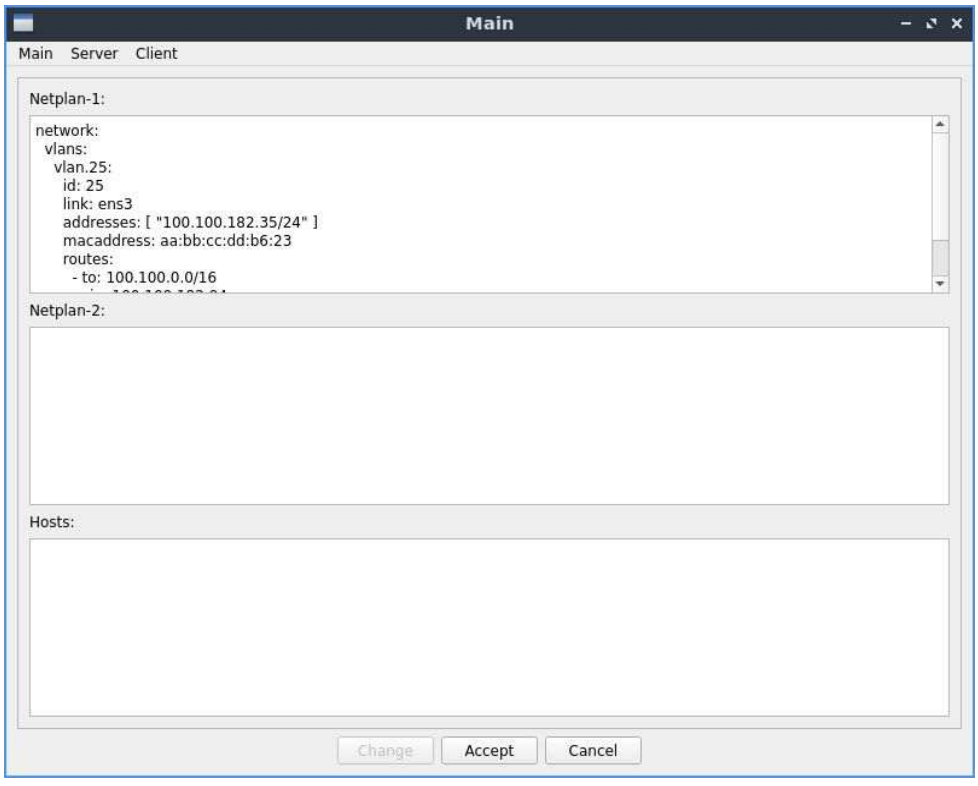

Рисунок 21 – Вкладка текущих параметров виртуальных сетевых адаптеров и списка доменных имен и соответствующих им адресов

На рисунке 19 приведен графический интерфейс главного окна. На данном рисунке изображена вкладка инструментария по наполнению базы данных физического описания сети MTD, данная вкладка доступна из выпадающего меню *Main* под пунктом *Device Manager*.

В этом же выпадающем меню доступны пункты *Settings*, где администратор может настроить параметры и сконфигурировать некоторые особенности функционирования предложенного метода: события реконфигурации (только через временные периоды, только по обнаружению злоумышленника, гибридный подход), диапазон меток групп, правила исключения, рандомизация (можно отключить рандомизацию, и случайные параметры будут конфигурироваться последовательно в соответствии с диапазонами допустимых значений) и многие другие.

На рисунке 20 приведен графический интерфейс вкладки, которая отражает текущую конфигурацию сети MTD. Данная вкладка доступна в выпадающем меню *Server* под пунктом *Engine*. В этом же выпадающем меню также доступны вкладки *NX-API Server*, *Host Server* и *VMTD Server*. Данные вкладки позволяют соответственно посмотреть обмен на уровне HTTP-клиента, посмотреть обмен на уровне WebSocket-сервера, а также посмотреть обмен и отправить собственные пользовательские запросы на уровне протоколов взаимодействия.

На рисунке 21 приведен графический интерфейс вкладки, которая отражает текущие параметры виртуальных сетевых адаптеров и список доменных имен и соответствующих им адресов. Данная вкладка доступна в выпадающем меню *Client* под пунктом *Configurator*.

В этом же выпадающем меню доступны вкладки *Host Client* и *VMTD Client*. Данные вкладки позволяют соответственно посмотреть обмен на уровне WebSocket-клиента, а также посмотреть обмен на уровне протоколов взаимодействия.

2.6 Выводы

1. Разработан 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. 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.

2. Для предложенного итерационного метода определен и описан объект защиты – локальная сеть передачи данных с топологией типа «звезда» или «дерево». В данной сети хосты неотличимы друг от друга и в ней не происходит никаких изменений на физических и канальных уровнях в рамках структурной взаимосвязи хостов.

3. Для объекта защиты определены потенциальные угрозы ИБ, связанные с исследованием сети. Актуальность этих угроз подтверждается публичными отчетами ведущих российских и зарубежных компаний в области ИБ: отмечается высокий уровень возникновения инцидентов, связанных с исследованием злоумышленниками локальных сетей передачи данных.

4. Составлена модель нарушителя, определены его возможности, а также рассмотрены его методы и средства по исследованию сети. Злоумышленник никак не ограничен в своих действиях, он может перемещаться по сети, перехватывать и анализировать сетевой трафик, а также сканировать хосты. Однако, он не осуществляет никаких деструктивных действий.

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 формирует одну новую работоспособную топологию из всех возможных топологий и сводит вероятность идентификации целевого хоста к $1/N$, где N – это количество хостов сети. Алгоритм формирования топологии сетевого уровня периодически заново используется для генерации новой топологии сетевого уровня, тем самым обеспечивая её постоянную реконфигурацию.

7. Для защиты локальной сети передачи данных от исследования злоумышленником и оценки эффективности на практике, предложенные метод и алгоритм были разработаны 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.

3. Анализ эффективности метода защиты локальной сети передачи данных от исследования на основе реконфигурации топологии сетевого уровня

3.1 Оценка на основе характеристик

Несмотря на высокий потенциал MTD, одной из серьезных проблем на пути ее широкого применения является отсутствие единой методологии оценки ее эффективности [78]. Отсутствие единой методологии оценки MTD приводит к несоответствиям в тестировании и сравнении решений MTD в различных средах.

По мере развития MTD были разработаны различные решения, каждое из которых обладает уникальными характеристиками. На основе работ [91, 96] выделены следующие характеристики, которые позволяют оценить эффективность решений MTD для защиты локальных сетей передачи данных от исследования злоумышленником:

1. подход к созданию пространства конфигураций;
2. схема управления;
3. подход к изменению параметров;
4. адаптивность;
5. разнообразность изменения поверхности атаки;
6. способ генерации параметров;
7. своевременность.

Защитники должны тщательно учитывать эти характеристики при выборе и развертывании MTD, чтобы убедиться, что они отвечают их потребностям ИБ без ущерба для функциональности ИС.

3.1.1 Подход к созданию пространства конфигураций

MTD обычно охватывает большое пространство конфигурации. Это пространство включает все возможные значения параметров, которые могут динамически изменяться в процессе функционирования MTD. По сути, это пространство определяет различные элементы, которые могут быть изменены

для обеспечения непредсказуемости. Каждое решение MTD включает в себя некоторое множество возможных конфигураций или состояний, которые может принять ИС, что обеспечивает постоянное изменение поверхности атаки и делает ИС непредсказуемой для потенциального злоумышленника.

Существует два подхода к созданию пространства конфигураций:

1. до начала процесса защиты (предопределенные конфигурации);

2. во время процесса защиты (конфигураций генерируемые «на лету»).

При подходе к созданию до начала процесса защиты все возможные конфигурации планируются заранее. Во время функционирования MTD выбирает конфигурацию из этого заранее определенного пространства, чтобы изменить поверхность атаки. Преимущества такого подхода:

1. Стабильность. MTD обеспечивает стабильное и предсказуемое пространство конфигураций. Это упрощает управление и мониторинг MTD, поскольку защитники могут заранее спланировать все возможные конфигурации, обеспечив их соответствие необходимым требованиям ИБ и производительности.

2. Ниже риск конфликтов конфигураций. Перед развертыванием предопределенные конфигурации могут быть протестированы на уязвимости и совместимость, что гарантирует, что ни одна конфигурация не внесет в ИС слабых мест.

3. Ниже вычислительные затраты. Поскольку MTD не нужно динамически генерировать новые конфигурации в процессе защиты, она не требует больших вычислительных ресурсов. В средах с ограниченными ресурсами, например, IoT, это может иметь решающее значение.

Недостатки такого подхода:

1. Единая точка отказа. При использовании предопределенных конфигураций, их необходимо хранить в каком-то хранилище, к которому может обращаться MTD. Этот подход создает предсказуемость и стабильность, но он также создает и единую точку отказа. Хранилище, где хранятся эти конфигурации, становится потенциальной целью для злоумышленника. Если это

хранилище будет скомпрометировано, злоумышленник сможет получить ценные данные о защитных механизмах и конфигурациях, а также сможет воздействовать на ИС путем модификации или уничтожения этих данных.

2. Предсказуемость. Существенным ограничением MTD, в которых формирование пространства конфигураций происходит в начале процесса защиты, является отсутствие гибкости. Злоумышленник, способный выявить закономерности или слабые места в предопределенных конфигурациях, может со временем использовать это в своих целях. Пространство предопределенных конфигураций конечно, и рано или поздно конфигурации могут повторяться. Таким образом, система становится предсказуемой.

К решениям MTD, в которых пространство конфигураций создается до начала процессы защиты, можно отнести только работу [128]. Наиболее распространен подход к созданию во время процесса защиты, которого придерживаются большинство решений в настоящий момент [91].

Преимущества такого подхода:

1. Непредсказуемость. Постоянно генерируя новые конфигурации, система остается непредсказуемой для злоумышленника. Он не может полагаться на разведывательные действия для выявления слабых мест, поскольку конфигурации всегда отличаются от предыдущих.

Недостатки такого подхода:

1. Выше риск конфликтов конфигураций. Генерация конфигураций «на лету» повышает риск возникновения конфликтов или нестабильности, особенно в сложных системах с множеством взаимодействующих компонентов.

2. Выше сложность управления и мониторинга. Управление динамичным пространством конфигураций может быть более сложным, требующим сложных инструментов мониторинга. Защитники должны убедиться, что конфигурации, которые генерирует MTD, не создают уязвимостей и не оказывают значительного негативного влияния на ИС.

3. Выше вычислительные затраты. Генерация конфигураций «на лету» требует несколько больше вычислительных ресурсов. Это может потенциально повлиять на производительность ИС.

В предложенном методе используется подход к созданию пространства конфигураций во время процесса защиты («на лету»).

3.1.2 Схема управления

Схема управления, используемая для контроля и координации защитных механизмов MTD, может существенно влиять на эффективность и общий уровень ИБ. В целом, схемы управления MTD можно разделить на:

1. централизованные;

2. децентрализованные;

3. частично централизованные.

Централизованное управление относится к схеме, в которой единый центральный объект отвечает за координацию и контроль всех действий MTD. Этот центральный объект собирает данные, принимает на их основе решения и распространяет конфигурации по всей ИС. Централизованная схема имеет ряд преимуществ:

1. Выше уровень координации. Централизованное управление позволяет получить единое представление о ИС и обеспечить последовательные и скоординированные изменения поверхности атаки. Такой подход может упростить принятие решений и повысить эффективность MTD, обеспечив согласованное внедрение изменений во всей ИС.

2. Упрощены мониторинг и аналитика. Централизованная система может собирать данные со всех частей ИС, что позволяет проводить всесторонний анализ потенциальных угроз и слабых мест. Собирая данные об атаках, централизованное управление может помочь выявить их закономерности.

Однако централизованная схема имеет ряд недостатков:

1. Единая точка отказа. Централизация управления создает единую точку отказа, которой может атаковать злоумышленник. Если центральный объект скомпрометирован, вся MTD может быть выведена из строя или подверг-

нута вредоносным воздействиям. Кроме того, централизованные системы могут страдать от проблем с масштабируемостью, поскольку одному объекту трудно эффективно управлять крупными распределенными ИС. Это может привести к задержкам при внедрении изменений, в результате чего отдельные части системы могут оказаться уязвимыми.

Большинство решений MTD имеют централизованную схему управления [91].

Децентрализованное управление, напротив, распределяет управление и контроль между несколькими объектами. Вместо того чтобы полагаться на центральный объект, каждый отдельный объект функционирует, принимая локальные решения, основанные на окружающей среде и ландшафте угроз. Преимущества такой схемы управления:

1. Масштабируемость и гибкость. Децентрализованные MTD могут легко расширяться, охватывая большие распределенные ИС, не испытывая при этом затруднений как в случае централизованного управления. Каждый объект может самостоятельно настраивать свою конфигурацию, что позволяет MTD быстрее реагировать на угрозы или изменения в среде. Благодаря этому децентрализованное управление особенно хорошо подходит для больших распределенных ИС, например, облачных платформ, где масштабная централизованная координация может быть неэффективной.

2. Устойчивость. Распределяя управление между несколькими объектами, MTD избегает проблемы единой точки отказа, присущей централизованным схемам. Даже если один объект скомпрометирован, остальная часть ИС может продолжать функционировать независимо.

К решениям MTD, которые имеют децентрализованную схему управления, можно отнести следующие работы [119, 131]. Работа [119] является попыткой реализации предложенного метода в децентрализованной схеме, однако данная реализация снижала пропускную способность до неприменимого уровня.

В ответ на ограничения централизованной и децентрализованной схем управления некоторые решения MTD используют частично централизованную схему. В такой схеме часть критичных функций управления и контроля выполняется централизовано, а часть – децентрализовано. Такая схема позволяет защитникам воспользоваться преимуществами масштабируемости и устойчивости децентрализованного управления, сохраняя при этом высокий уровень координации и мониторинга, обеспечиваемый централизованным управлением. Однако такая схема гораздо сложнее в реализации. К решениям MTD, которые используют частично централизованную схему управления, можно отнести работу [131].

В предложенном методе используется централизованная схема управления.

3.1.3 Подход к изменению параметров

Важнейшим аспектом MTD является подход к изменению параметров:

1. изменение реальных значений параметров;

2. подмена реальных значений параметров фиктивными.

Изменение реальных значений параметров подразумевает периодическое изменение, чтобы сделать ранее собранную злоумышленником информацию недействительной. Преимущества такого подхода:

1. злоумышленник сталкивается с постоянно изменяющейся поверхностью атаки.

Недостатки такого подхода:

1. необходима синхронизация между элементами MTD во избежание отказов в обслуживании;

2. может снижаться производительность из-за частой смены конфигураций.

Подмена фиктивными значениями подразумевает создание в ИС ложной информации, чтобы ввести в заблуждение злоумышленника. В отличие от изменения реальных значений, этот подход сохраняет исходные параметры

неизменными, создавая при этом ложные значения, которые кажутся злоумышленнику достоверными. Преимущества такого подхода:

1. сохраняет целостность рабочих параметров, при этом вводя злоумышленников в заблуждение;

2. не снижает производительность сети из-за смен конфигураций.

Недостатки такого подхода:

1. злоумышленник может распознать и проигнорировать фиктивные значения.

В решениях MTD, в настоящее время, активно применяются оба подхода [91]. Примером решения, которое использует изменение реальных значений, являются работы [92б 118], а которое использует подмену фиктивными значениями – работы [96, 116, 117].

3.1.4 Адаптивность

Одним из компонентов, который повышает эффективность MTD, является механизм адаптации. Механизм адаптации позволяет MTD реагировать и подстраиваться под изменяющиеся угрозы или среду, то есть менять конфигурации в режиме реального времени так, чтобы нейтрализовать угрозу, например, перенаправив трафик. Это снижает вероятность успешного использования уязвимостей злоумышленником, поскольку MTD развивается быстрее, чем злоумышленник успевает скорректировать свою тактику. Без механизмов адаптации MTD хоть и изменяет поверхность атаки, но делает это без учета текущего ландшафта угроз или состояния ИС. Примером решения с адаптивностью является работы [118, 132]. Большинство же решений, полагаются на то, что злоумышленник воспользуется устаревшей или ложной информацией и тем самым демаскирует себя [91]. Предложенный метод имеет механизмы по изоляции злоумышленника в случае его обнаружения, т.е. обладает адаптивностью.

3.1.5 Разнообразность изменения поверхности атаки

Решения MTD можно разделить в зависимости от механизмов, которые они используют для создания динамичной и непредсказуемой среды: от про-

стых, которые заключаются в смене IP-адресов и портов, до сложных, в основе которых лежит реконфигурация топологии сети в совокупности с динамичностью на уровне ПО. Чем больше параметров изменяет MTD, тем выше уровень защищенности объекта защиты, потому что MTD изменяет поверхность атаки злоумышленника более разнообразно. Предложенный метод манипулирует физическими и логическими адресами, маршрутами передачи данных и логической топологией сети MTD, в отличие от других решений, которые манипулируют более ограниченным набором параметров [91].

3.1.6 Способ генерации параметров

Непредсказуемость является важной характеристикой MTD. MTD затрудняет злоумышленнику предсказание точной информации об атакуемой ИС на каждой следующей конфигурации, тем самым увеличивая трудозатраты на атаку и снижая вероятность успешной атаки, тем самым повышая защищенность атакуемой ИС.

В механизмах MTD под непредсказуемостью обычно понимается случайность, которая является внешним проявлением способа выбора следующей конфигурации или, точнее, способа генерации параметров. Случайность означает то, что защитники выбирают следующую конфигурацию случайно с точки зрения злоумышленника, что приводит к непредсказуемости MTD. Поэтому непредсказуемость является ключевым фактором, обеспечивающим эффективность MTD.

Почти все решения MTD обладают этим свойством, и разница между ними заключается в способе генерации параметров. Существуют следующие способы генерации параметров [91]:

1. случайности;
2. машинное обучение;
3. хэш-функция;
4. предопределенные стратегии;
5. стратегии, построенные на теории игр и марковских процессах.

Предложенный метод использует случайности.

3.1.7 Своевременность

Ограниченная своевременность – это важнейшая характеристика MTD, поскольку оно напрямую влияет на временное окно, которое есть у злоумышленника для реализации атаки. Частое изменение параметров значительно сокращает длительность времени актуальности любой информации, собранной злоумышленником.

Своевременность может быть ограничена:

1. фиксированным периодом;
2. динамическим периодом;
3. наступлением события.

Фиксированные периоды смены конфигурации обеспечивают предсказуемый график, которым легче управлять, но в конечном итоге злоумышленник может предугадать его, если будет наблюдать за MTD в течение долгого времени. Динамические периоды, с другой стороны, вносят непостоянство, что усложняет задачу злоумышленника по предсказанию времени смены конфигурации, но они могут потребовать более сложного управления, чтобы избежать ненужных сбоев в легитимной работе сети.

Некоторые решения MTD могут менять конфигурации по наступлению событий, например, обнаружение подозрительной активности или возникновение инцидентов. Такой подход гарантирует, что MTD динамически реагирует на потенциальные угрозы, активируя защиту именно тогда, когда это необходимо. Однако этот подход зависит от точности механизмов обнаружения, поэтому могут либо пропустить угрозы, либо вызвать избыточные изменения, что повлияет на производительность сети.

В продвинутых решениях MTD может использоваться гибридный подход, сочетающий фиксированные или динамические периоды с событийными триггерами, чтобы сбалансировать предсказуемость и своевременность.

В конечном счете своевременность заключается в том, чтобы любые данные, которые собирает злоумышленник, устаревали до того, когда их

можно будет использовать для атаки. В результате увеличивается сложность и стоимость проведения атаки.

Все подходы активно используются в решениях MTD [91]. В предложенном методе своевременность ограничена фиксированным периодом и наступлением события.

Теперь необходимо экспериментально оценить накладные расходы для обеспечения тех характеристик, которые имеет предложенный метод, при помощи предложенного алгоритма и программного средства.

3.2 План эксперимента

Эффективность MTD также оценивается с помощью метрик, которые отражают «плату» производительностью ИС за имеющиеся характеристики.

3.2.1 Анализ публикаций по оценке эффективности на основе метрик

На основе работ [84, 91, 92] выделены следующие метрики, которые позволяют оценить накладные расходы решений MTD для защиты локальных сетей передачи данных от исследования злоумышленником:

1. нагрузка на сетевое оборудование;
2. накладные расходы адресного пространства;
3. накладные расходы на передачу;
4. накладные расходы на маршрутизацию;
5. пропускная способность;
6. потери пакетов;
7. задержки.

3.2.2 Параметры эксперимента

Для экспериментальной оценки эффективности предложенного метода на основе метрик был создан стенд в виртуальной среде EVE-NG. Так как сеть разворачивается внутри виртуальной лаборатории EVE-NG, её структура и наполнение ограничена количеством ресурсов. Для того, чтобы избежать значительного снижения производительности из-за выгрузки данных из оперативной памяти на твердотельный накопитель и обратно, необходимо всю

сеть поместить в объем оперативной памяти. Характеристики ПК, на котором размещена виртуальная лаборатория EVE-NG, представлены в таблице 4.

Таблица 4 – Основные характеристики ПК тестового стенда

Характеристика	Значение
Процессор	Ryzen 9 5900x 12 ядер 24 потока 3,7-4,8 ГГц архитектура Zen 3
Оперативная память	2 x 16 ГБ DDR4 3200 МГц
Операционная система	Windows 10 22H2 x64

Весь объем оперативной памяти составляет 32 ГБ. Объем, требуемый для ОС самого ПК, составляет 2 ГБ. Также необходимо выделить память для самой виртуальной лаборатории EVE-NG составляет 4 ГБ, включая ОС самого ПК. Требуемый объем оперативной памяти для одного L3 Cisco Nexus коммутатора составляет 8 ГБ. Так как требуется проверить управление несколькими сетевыми устройствами, их требуется, как минимум, два. Требуемый объем оперативной памяти для одного хоста составляет 1 ГБ. Таким образом, сетевая инфраструктура состоит из 2 коммутаторов и 12 хостов. Схема стенда приведена на рисунке 19.

Испытания следует проводить следующим образом. Всего необходимо осуществить пять испытаний:

1. Без реконфигурации сети.
2. С реконфигурацией сети с периодом равному критичному.
3. С реконфигурацией сети с периодом меньше критичного на 25 %.
4. С реконфигурацией сети с периодом меньше критичного на 50 %.
5. С реконфигурацией сети с периодом меньше критичного на 75 %.

Длительность каждого испытания – 15 минут, что является стандартом длительности тестирования сетей локального масштаба [124]. Инструкция по развертыванию тестового стенда приложена в репозитории проекта [113].

Критичный период, по своей сути, это то время, которое необходимо злоумышленнику для сбора информации о сети и перехода на следующую стадию реализация атаки. Период больше критичного приведет к тому, что

злоумышленник сможет атаковать ИС, так как уже собрал информацию о ней, при этом информация будет актуальной, пусть и определенный период времени. Период меньше критичного не только приведет к тому, что после стадии разведки собранная информация устареет, но и ограничит объем информации, который успеет собрать злоумышленник за одну конфигурацию. Поэтому необходимо оценить, какое влияние оказывает сокращение периода функционирования одной конфигурации на накладные расходы.

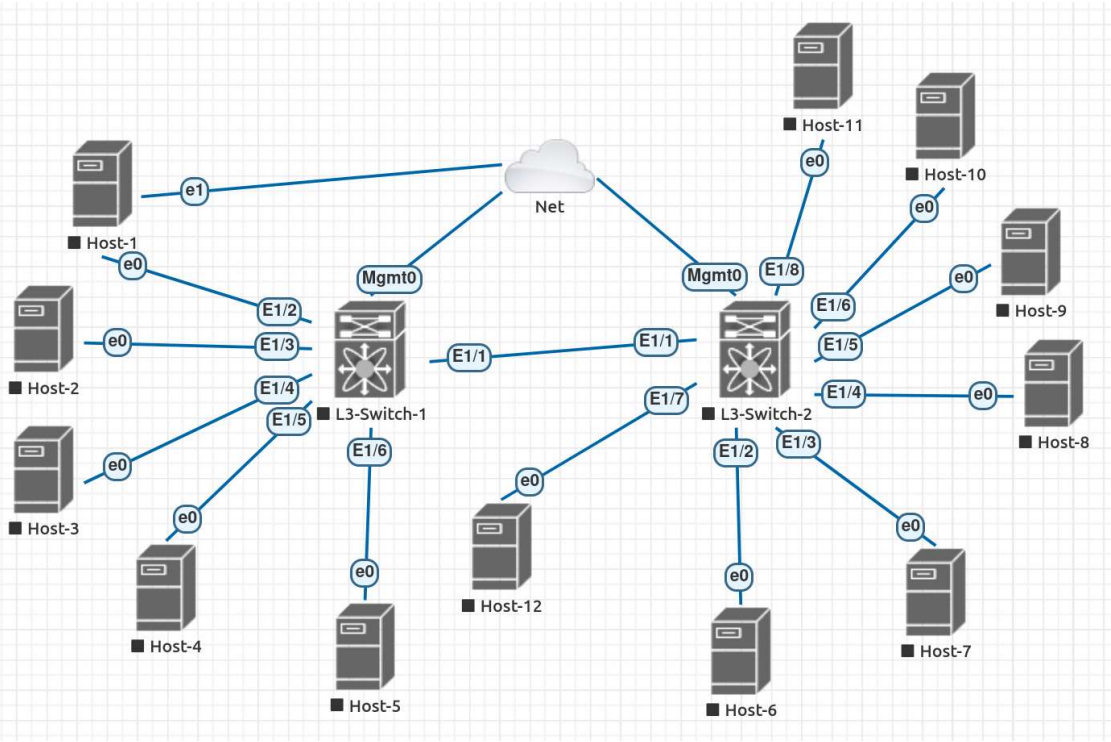

Рисунок 19 – Схема тестового стенда

3.3 Оценка на основе метрик

На каждом периоде проведены измерения метрик, правила проведения которых приведены в соответствующих разделах.

3.3.1 Нагрузка на сетевое оборудование

Оценка влияния MTD на нагрузку сетевого оборудования необходима для понимания ее практических последствий для производительности сети. MTD вводит дополнительные механизмы, которые могут увеличить нагрузку на коммутаторы и маршрутизаторы. Это может привести к перегрузке сети,

если оборудование не способно справиться с дополнительной вычислительной нагрузкой, необходимой для постоянной реконфигурации.

Необходимость в такой оценке обусловлена тем, что MTD добавляет сложность в обычные сетевые операции. Частые изменения конфигурации могут привести к увеличению нагрузки на процессор и потреблению памяти. Перегрузка сетевого оборудования может снизить общую производительность сети, что приведет к замедлению обмена данными и снижению качества обслуживания.

Оценка того, как MTD влияет на нагрузку на сетевое оборудование, необходима, чтобы защитники, внедряющие MTD, не создали «узкие места» в производительности из-за перегруженности оборудования. Такая оценка поможет определить, требуется ли модернизация оборудования или оптимизация MTD для её функционирования без ущерба для производительности сети.

За весь период тестирования нагрузка на процессор коммутатора и потребление оперативной памяти составила в пределах до 40 % для процессора и до 20 % для памяти.

3.3.2 Накладные расходы адресного пространства

В контексте MTD под адресным пространством понимается диапазон IP-адресов, которые используются для создания подвижных целей. Динамические изменения в адресном пространстве затрудняют злоумышленнику поддержание последовательного представления о сети, тем самым эти изменения снижают вероятность успешной атаки. Однако эффективность этого снижения MTD напрямую связана с размером и вариативностью адресного пространства, которое может быть занято MTD.

Накладные расходы адресного пространства MTD относятся к дополнительным ресурсам, которые требуются для постоянного изменения поверхности атаки. Оценка накладных расходов адресного пространства важна, поскольку они влияют на масштабируемость и устойчивость MTD. Если накладные расходы адресного пространства слишком велики, это может при-

вести к исчерпанию ресурсов и, возможно, сделает MTD неприменимой для долгосрочного использования.

Оценка накладных расходов адресного пространства позволяет защитникам более эффективно планировать распределение адресов в сети, обеспечивая наличие их достаточного количества для поддержания MTD без ущерба для других сетевых операций. Оценка накладных расходов адресного пространства также позволяет защитникам определить, может ли их текущая инфраструктура поддерживать MTD или необходим переход на сеть с бóльшим адресным пространством. Такая оценка особенно важна в облачных средах, где динамическое распределение ресурсов может значительно увеличить стоимость и сложность управления, если не спланировать все должным образом.

Предложенный метод имеет следующие накладные расходы на адресное пространство. В текущей программной реализации предложенного алгоритма выделена подсеть с маской 16, то есть всего поддерживается не более 65534 адресов. Предложенный метод может функционировать и на более ограниченном адресном пространстве, однако, чем меньше выделено адресного пространства, тем меньше нужно времени злоумышленнику для его исследования. Также с уменьшением адресного пространства сеть становится предсказуемой, так как уменьшается выборка адресов для исследования.

3.3.3 Накладные расходы на передачу

Оценка накладных расходов на передачу данных в контексте MTD важна для обеспечения приемлемой производительности сети, оптимизации распределения ресурсов и поддержания общей эффективности. Накладные расходы на передачу в MTD заключаются в дополнительных данных, которые передаются по сети для поддержания функционирования MTD. Сюда относятся следующие накладные расходы: дополнение пакетов новыми заголовками или данными, обновление таблиц маршрутизации, передача новых конфигураций или информации о состоянии сети. Эти операции необходимы для обеспечения подвижности целей, но они могут негативно влиять на производительность передачи данных.

Кроме того, оценка накладных расходов на передачу имеет важное значение для оптимизации MTD. Понимая, в каких именно областях возникают накладные расходы, исследователи могут определить возможности для оптимизации операций и сокращения избыточной передачи данных.

Для оценки накладных расходов на передачу использовался инструмент для анализа сетевого трафика Wireshark. Эксперимент проводился следующим образом. В течение всего периода тестирования, который включает в себя все испытания, собирался дамп трафика на сетевых адаптерах участника-сервера, через которые он осуществляет управление сетью MTD. После чего собранный трафик анализировался путем сбора статистической информации о содержимом пакетов и их размерах.

Реализация предложенного алгоритма никак не модифицирует передаваемые по сети пакеты данных. Участник-сервер передает и принимает: управляющие команды сетевому оборудованию; параметры виртуальных сетевых адаптеров и списки доменных имен и соответствующих им адресов каждому участнику взаимодействия; списки потенциально опасных хостов от каждого участника. По причине того, что протокол JSON RPC 2.0 является символьным, размер каждого сетевого пакета зависит от количества символов в JSON-объекте, а данные, которыми наполняются эти JSON-объекты, не имеют фиксированную длину. Поэтому оценка накладных расходов на передачу является приблизительной и должна быть оценена в каждом отдельном случае. Точные значения размеров сетевых пакетов, приведенных в данном разделе, отличаются на каждой реконфигурации незначительно. Сетевые пакеты, которые содержат один и тот же набор данных, но отличаются друг от друга непосредственно самими данными, в среднем отличаются друг от друга на величину от 0 до 12 символов. Один символ кодируется 2 байтами. Все размеры указаны на уровне фреймов.

Размер одного сетевого пакета, содержащего управляющие команды для одного сетевого устройства, зависит от количества настраиваемых интерфейсов и меток. В среднем для данного тестового стенда, размер пакета,

предназначенного для установки соединения с одним сетевым устройством и его конфигурирования, составляет 8416 байт.

Размер одного сетевого пакета, содержащего параметры виртуального сетевого адаптера участника взаимодействия без маршрутов, составляет в среднем 268 байт, с одним маршрутом – 510 байт, а каждый последующий маршрут увеличивает в среднем размер пакета на 76 байт. Такой пакет передается каждому участнику взаимодействия при каждой смене топологии сетевого уровня. Ответ на такой пакет имеет среднюю длину 132 байта.

Размер одного сетевого пакета, содержащего команду на очистку параметров виртуального сетевого адаптера, составляет 165 байт.

Размер одного сетевого пакета, содержащего список из одного доменного имени и соответствующего ему адреса, в среднем составляет 234 байта при длине доменного имени 9 символов. Размер этого пакета в значительной степени зависит от длины доменного имени. Каждое последующее доменное имя такой длины и соответствующий ему адрес увеличивают размер пакета на 177 байт. Такой пакет отправляется каждому участнику взаимодействия при каждой реконфигурации топологии сетевого уровня. Ответ на такой пакет имеет среднюю длину 132 байта.

Размер одного сетевого пакета, который содержит команду на установку новых параметров, составляет 162 байта.

Помимо распространения участником-сервером параметров участники взаимодействия рассылают списки потенциально опасных хостов. Размер одного сетевого пакета, который содержит информацию об одном потенциально опасном хосте, составляет в среднем 286 байт. Каждый последующий потенциально опасный хост увеличивает в среднем размер пакета на 54 байта. Данные пакеты рассылаются либо по запросу от участника-сервера, либо по обнаружению злоумышленника, поэтому частота рассылки зависит от возникновения этих событий. Если эти события не возникают, то и информация о потенциально опасных хостах не распространяется.

Для данного тестового стенда на одну реконфигурацию на одного участника взаимодействия при наличии у каждого участника доменного имени из 9 символом без оповещений и запросов списков потенциально опасных хостов в среднем пришлось 3600 байт.

Итого в среднем на одну реконфигурацию для данного тестового стенда требуется 67232 байт. Итоговый подсчет осуществлялся путем сложения размеров пакетов, связанных с IP-адресами участников взаимодействия и сетевых устройств.

3.3.4 Накладные расходы на маршрутизацию

Хотя MTD значительно повышает сложность и стоимость атаки для потенциального злоумышленника, MTD также вводит дополнительные накладные расходы на маршрутизацию. Для достижения максимальной производительности передачи данных, пакеты должны доставляться по кратчайшим маршрутам. Очевидно то, что для достижения непредсказуемости MTD необходимо отклоняться от кратчайших маршрутов.

Периодичное изменение таблиц маршрутизации приводит к временным сбоям, пока сеть сходится на новых путях маршрутизации. В результате этих проблем пакеты данных могут задерживаться, отбрасываться или направляться по неоптимальным путям, что приводит к увеличениям задержек и к потере пакетов. Эти проблемы могут негативно повлиять на чувствительные к задержкам приложения.

В MTD маршруты часто меняются для того, чтобы злоумышленник не мог определить или предугадать топологию сети. Эти изменения могут привести к тому, что пакеты данных будут проходить до места назначения более длинными маршрутами. В MTD маршруты намеренно удлиняются и содержат множество промежуточных переходов, чтобы скрыть истинную топологию сети и добиться её непредсказуемости.

Масштабируемость MTD также зависит от накладных расходов, связанных с маршрутизацией. В небольших сетях влияние накладных расходов на маршрутизацию может быть незначительным. Однако по мере роста раз-

мера и сложности сети эффект от изменения маршрутов MTD может стать значительным.

Для оценки накладных расходов на маршрутизацию использовался инструмент для определения маршрутов следования данных traceroute. В сети было выбрано два случайных хоста, для которых определялся маршрут следования данных на каждой итерации реконфигурации. Происходило это в течение всего периода тестирования. За время тестирования было совершено 27 реконфигураций. Результаты накладных расходов для данного тестового стенда приведены в таблице 5.

Таблица 5 – Испытания по оценке накладных расходов на маршрутизацию

Конфигурация									
№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	№ 7	№ 8	№ 9	№ 10
0	11	9	8	0	7	4	2	5	9
Конфигурация									
№ 11	№ 12	№ 13	№ 14	№ 15	№ 16	№ 17	№ 18	№ 19	№ 20
8	3	1	0	4	10	5	7	6	2

Минимальная длина маршрута составила 0 переходов. Максимальная длина маршрута составила 9 переходов. Средняя длина маршрута составила 4 перехода. Для произвольного числа участников максимальная длина маршрута составит $N-1$ переходов, где N – число участников взаимодействия. Средняя длина маршрута во многом зависит от генератора случайных чисел. В данном случае использовался генератор, поставляемый фреймворком Qt, а именно – *QRandomGenerator::global()*.

3.3.5 Пропускная способность

Частые изменения поверхности атаки могут привести к снижению пропускной способности, увеличению задержек и потере пакетов, что может негативно повлиять на работу приложений, которые зависят от высокой стабильности и производительности соединений. Если накладные расходы слишком велики, сеть может не справиться с постоянными изменениями, требуемыми MTD, что приведет к снижению качества обслуживания.

Пропускная способность – это ключевая метрика производительности, которая отражает эффективность передачи данных в сети. Предложенный метод влияет на пропускную способность частыми изменениями логической топологии сети, маршрутов и других параметров. Измерение пропускной способности имеет важное значение для оценки влияния MTD на производительность передачи данных и, как следствие, обеспечение того, чтобы MTD не наносило значительный ущерб производительности.

Одной из основных проблем при внедрении MTD является поиск оптимального баланса между уровнем ИБ и производительностью передачи данных. Измеряя пропускную способность, защитники могут оценить негативное влияние MTD на производительность сети, и соответствующим образом скорректировать ее механизмы. Например, если измерения пропускной способности показывают значительное снижение в периоды высокой активности, возможно, необходимо доработать MTD так, чтобы уменьшить частоту или масштаб изменений.

Для оценки использовался инструмент для тестирования пропускной способности сети iperf3. Замеры производились следующим образом. Сервер был запущен при помощи команды: *iperf -s -u -i 1*. Клиент был запущен при помощи команды: *iperf -c <IP-адрес сервера> -u -t 900 -b 10m*. Получены следующие результаты (рисунки 20-23):

1. Измерение пропускной способности без реконфигурации сети (рисунок 20). Средняя пропускная способность за период составила 9,99 Мбит/с.

2. Измерение пропускной способности с реконфигурацией сети с периодом 400 секунд (рисунок 21). Средняя пропускная способность за период составила 8,93 Мбит/с. Снижение от результатов без реконфигурации сети составило 10 %.

3. Замер пропускной способности с реконфигурацией сети с периодом 300 секунд (рисунок 22). Средняя пропускная способность за период составила 8,98 Мбит/с. Снижение от результатов без реконфигурации сети составило 31 %.

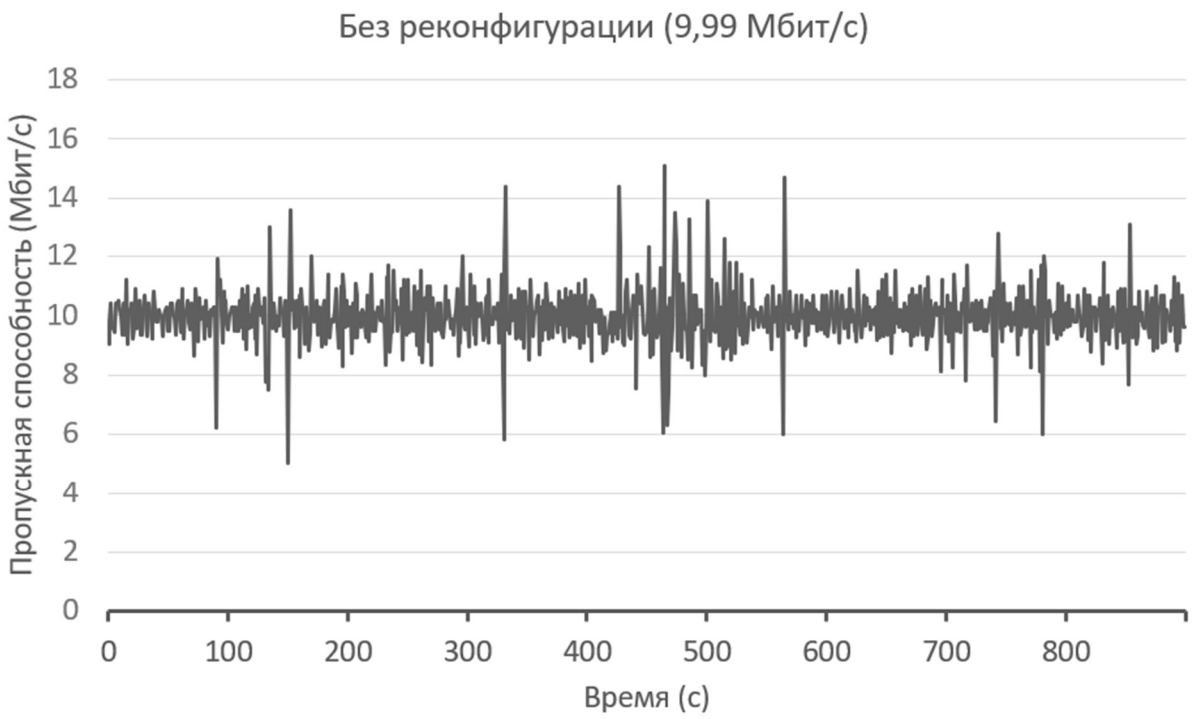

Рисунок 20 – Результаты измерения пропускной способности (Мбит/с) без реконфигурации сети

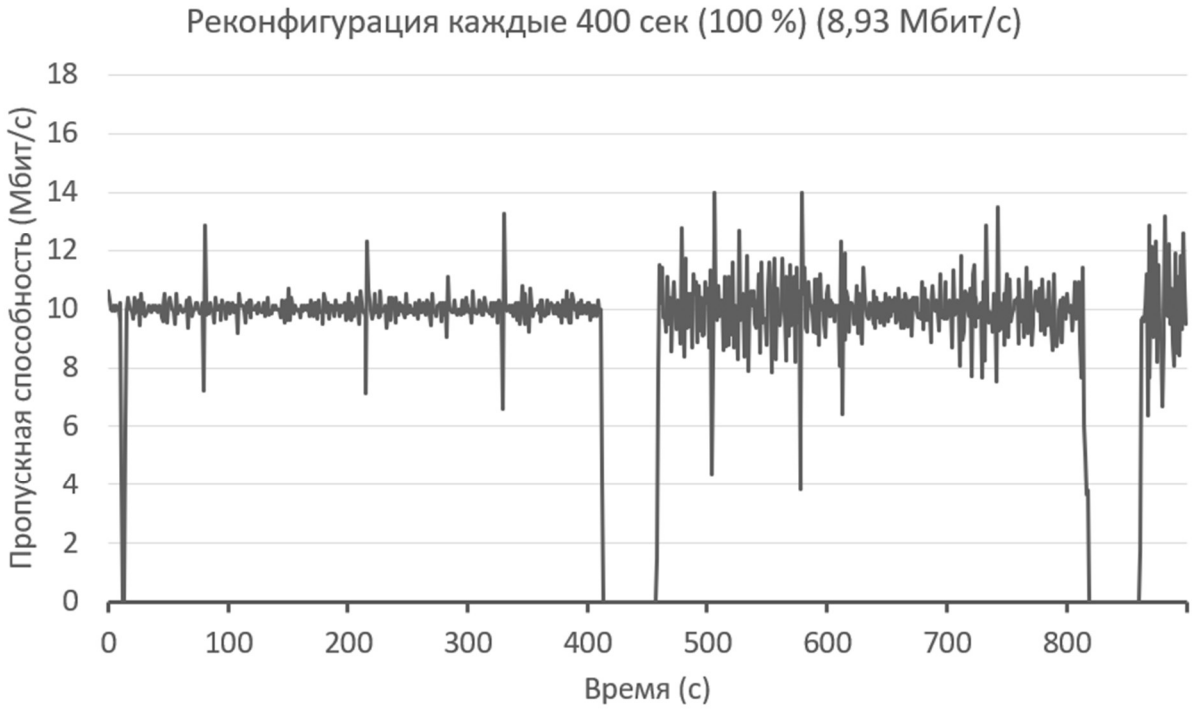

Рисунок 21 – Результаты измерения пропускной способности (Мбит/с) с реконфигурацией сети каждые 400 секунд

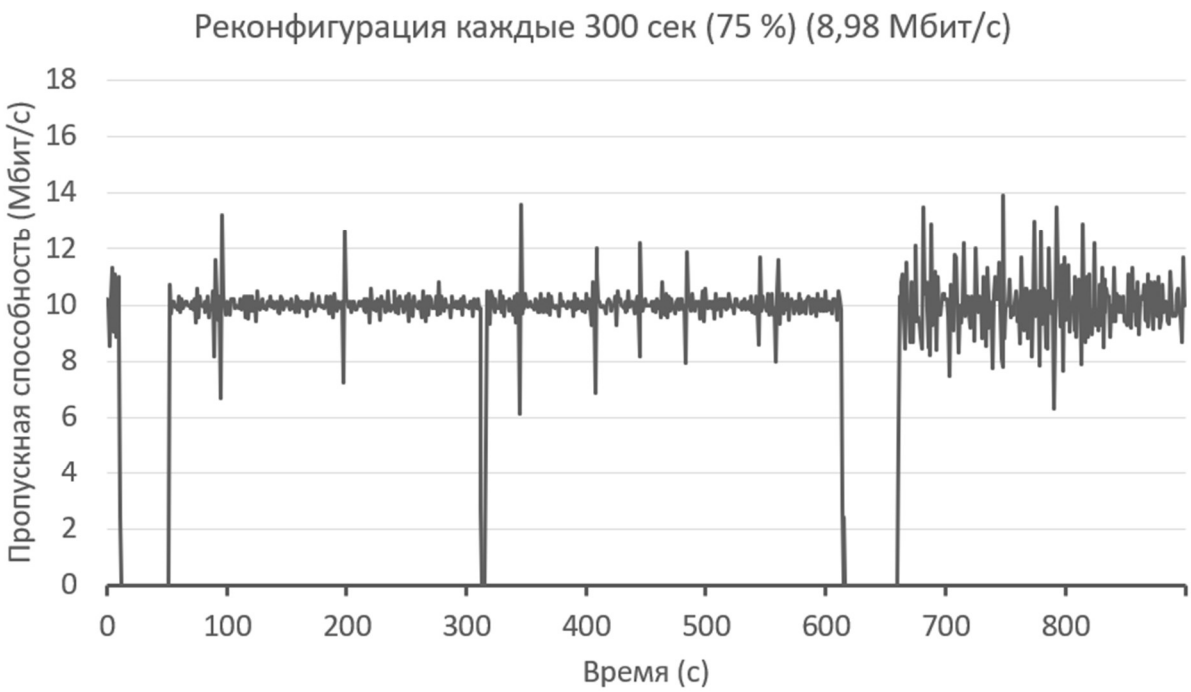

Рисунок 22 – Результаты измерения пропускной способности (Мбит/с) с реконфигурацией сети каждые 300 секунд

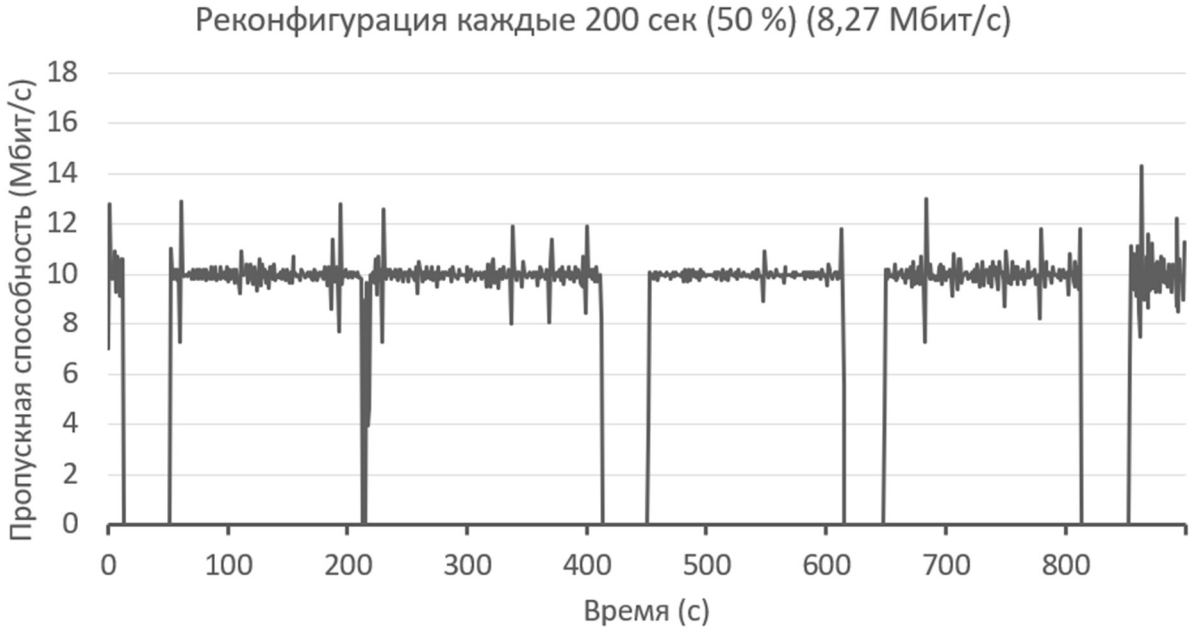

Рисунок 23 – Результаты измерения пропускной способности (Мбит/с) с реконфигурацией сети каждые 200 секунд

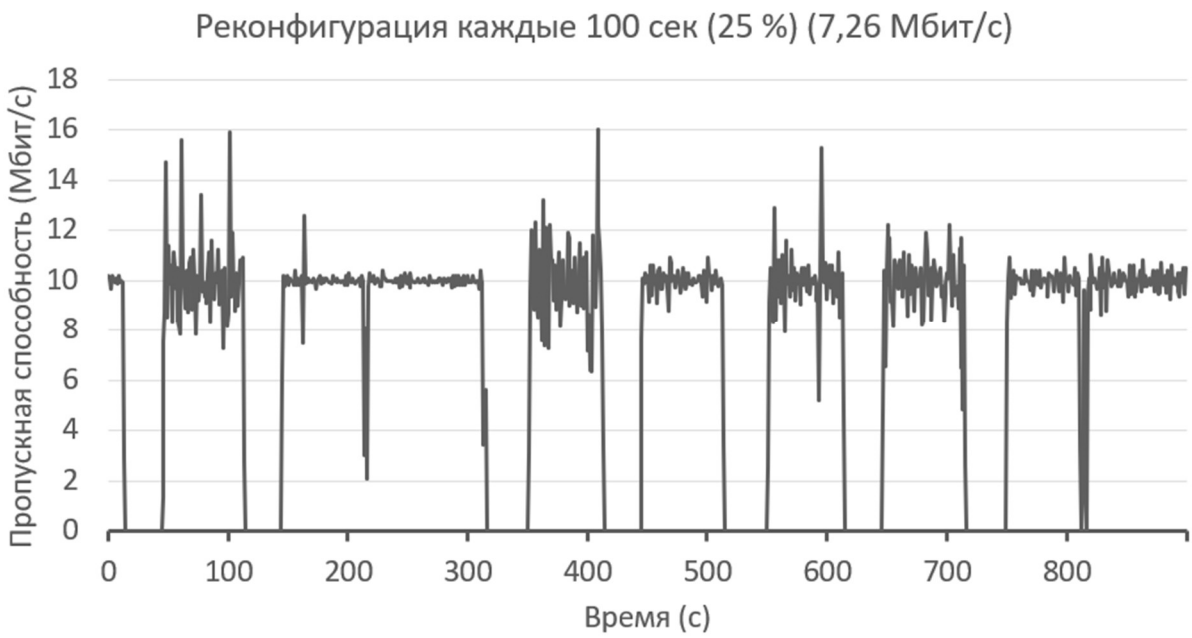

Рисунок 24 – Результаты измерения пропускной способности (Мбит/с) с реконфигурацией сети каждые 100 секунд

4. Замер пропускной способности с реконфигурацией сети с периодом 200 секунд (рисунок 23). Средняя пропускная способность за период составила 8,27 Мбит/с. Снижение от результатов без реконфигурации сети составило 18 %.

5. Замер пропускной способности с реконфигурацией сети с периодом 100 секунд (рисунок 24). Средняя пропускная способность за период составила 7,26 Мбит/с. Снижение от результатов без реконфигурации сети составило 27 %.

3.3.6 Потери пакетов

Измерение потерь пакетов имеет важное значение для понимания влияния MTD на надежность сети и обеспечения того, чтобы MTD не оказало значительного снижения качества обслуживания.

Потеря пакетов может быть вызвана различными факторами, включая перегрузку сети, ошибки при передаче или сбои в маршрутизации. MTD создает периоды нестабильности из-за изменений топологии или путей маршрутизации, пока сеть адаптируется к новым конфигурациям. Во время таких

переходов пакеты могут быть потеряны, что приводит к снижению качества обслуживания.

Оценка потерь пакетов дает защитникам ценную информацию о том, насколько эффективно работает MTD. Если потеря пакетов окажется неприемлемо высокой, это может свидетельствовать о том, что частота или масштаб изменений в сети слишком высоки. Анализируя данные о потере пакетов, защитники могут скорректировать MTD, чтобы найти оптимальный баланс между уровнем ИБ и производительностью, обеспечивая приемлемые значения.

Для оценки потери пакетов также использовался инструмент для тестирования пропускной способности сети iperf3 и на основе тех же периодов (рисунки 24-27):

1. Измерение потерь пакетов без реконфигурации сети (рисунок 25). Потери за период составили 584 пакета из 765306 (0.076 %).

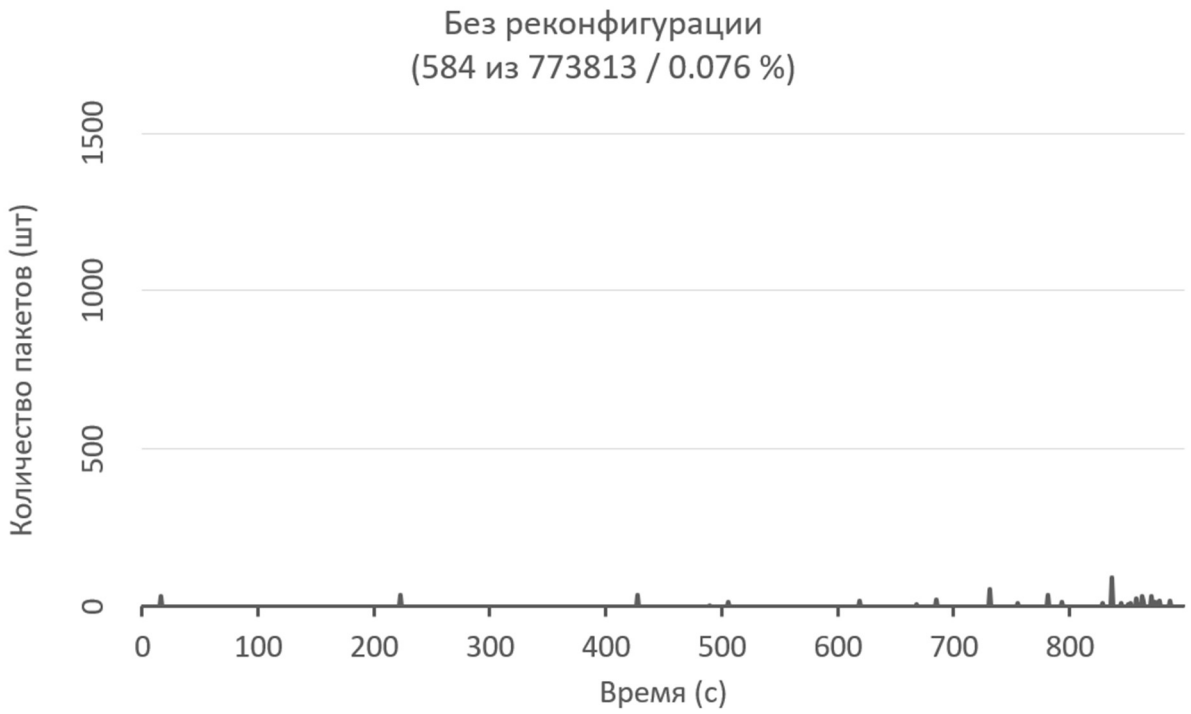

Рисунок 25 – Результаты измерения потерь пакетов без реконфигурации сети

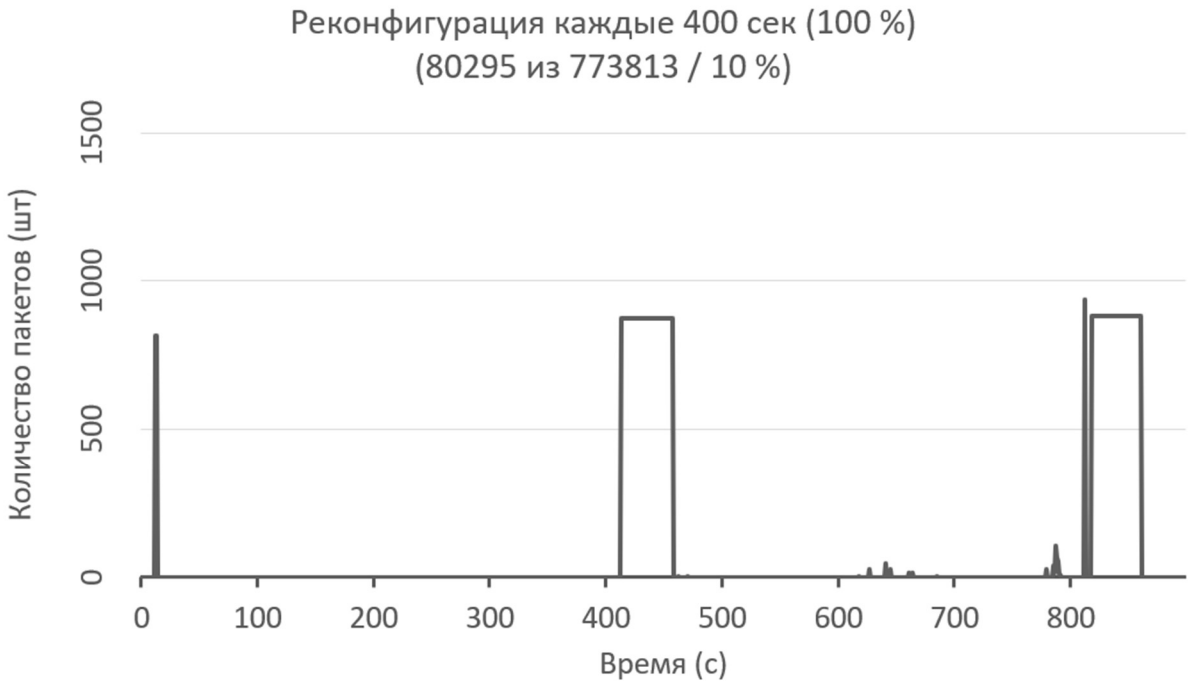

Рисунок 26 – Результаты измерения потерь пакетов с реконфигурацией сети каждые 400 секунд

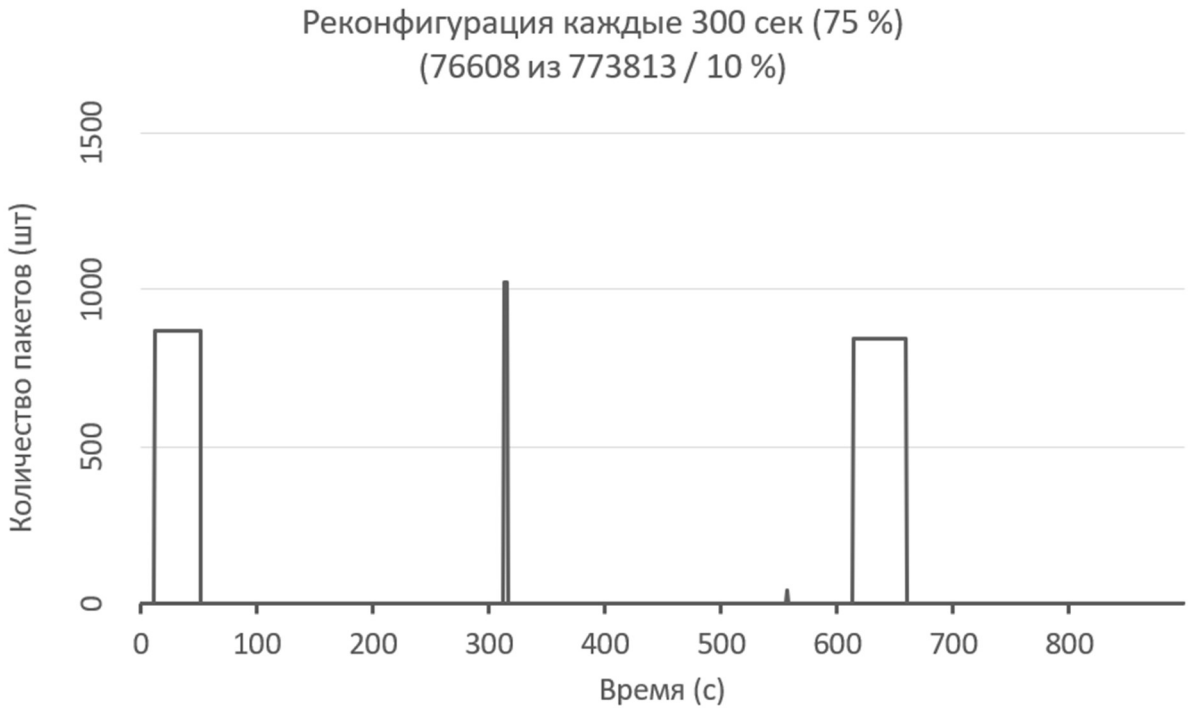

Рисунок 27 – Результаты измерения потерь пакетов с реконфигурацией сети каждые 300 секунд

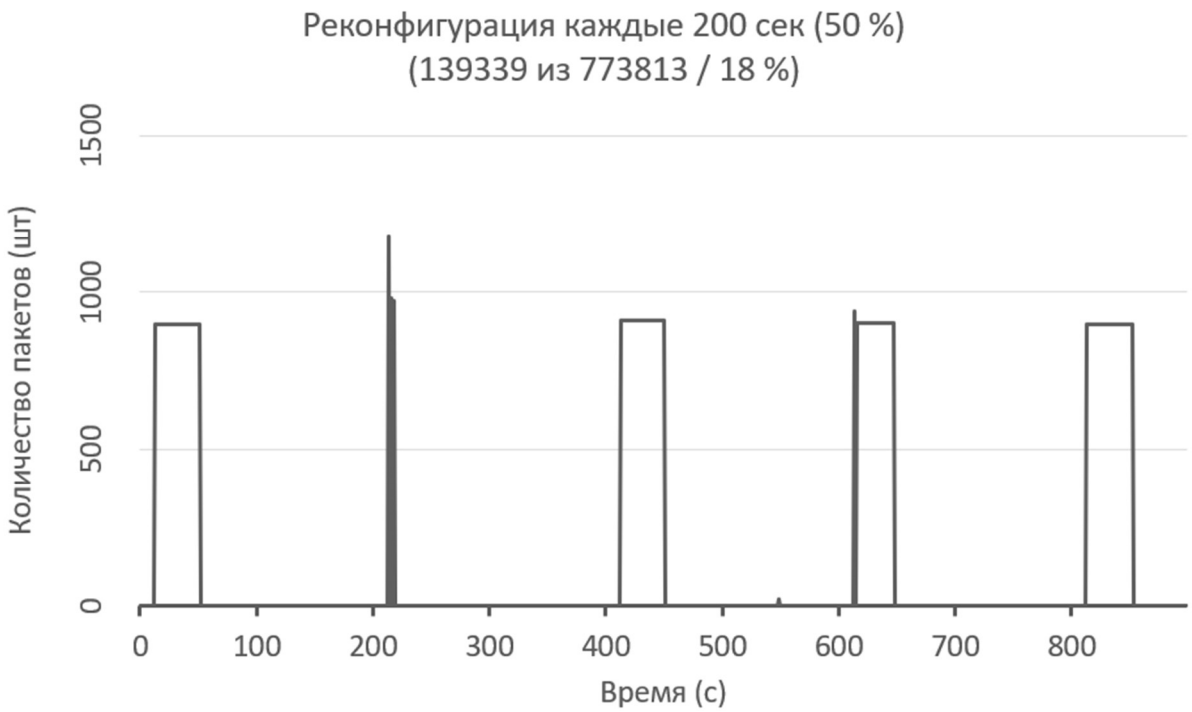

Рисунок 28 – Результаты измерения потерь пакетов с реконфигурацией сети каждые 200 секунд

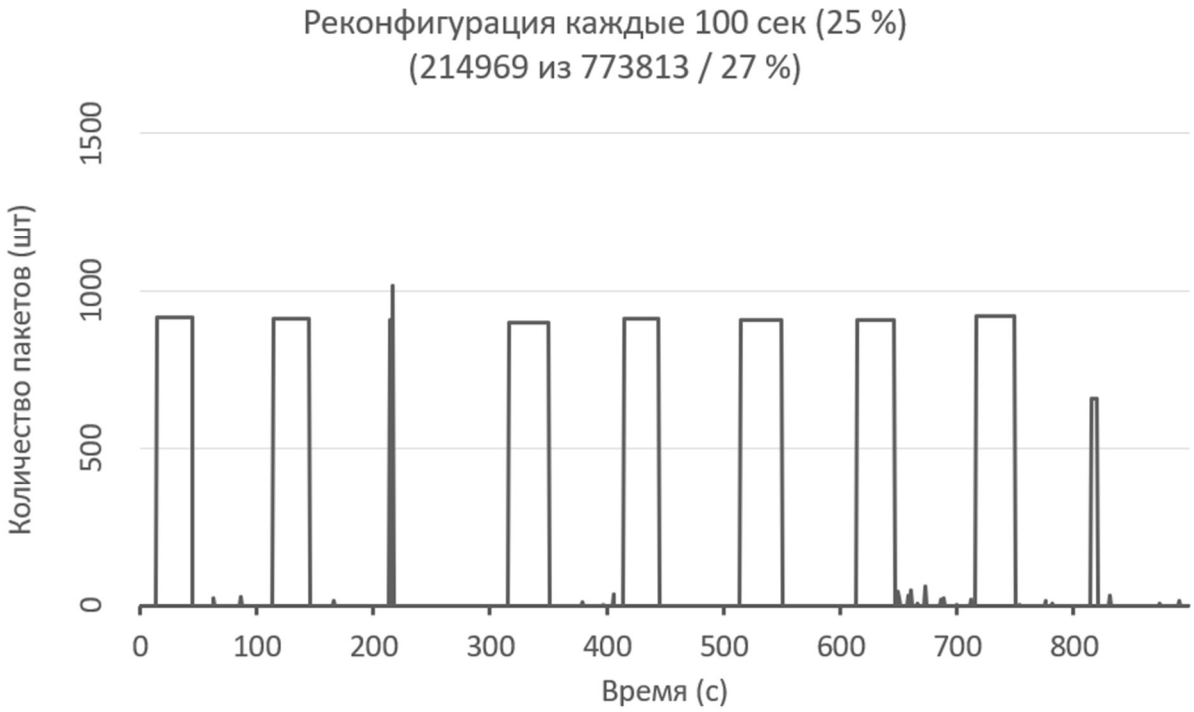

Рисунок 29 – Результаты измерения потерь пакетов с реконфигурацией сети каждые 100 секунд

2. Измерение потерь пакетов с реконфигурацией сети с периодом 400 секунд (рисунок 26). Потери за период составили 80295 пакетов из 773813 (10 %).

3. Измерение потерь пакетов с реконфигурацией сети с периодом 300 секунд (рисунок 27). Потери за период составили 76608 пакета из 773813 (10 %).

4. Измерение потерь пакетов с реконфигурацией сети с периодом 200 секунд (рисунок 28). Потери за период составили 139339 пакета из 773813 (18 %).

5. Измерение потерь пакетов с реконфигурацией сети с периодом 100 секунд (рисунок 29). Потери за период составили 214969 пакета из 773813 (27 %).

3.3.7 Задержки

Задержки показывают время, которое требуется пакету данных, чтобы добраться от источника до получателя. В сети, где применяется MTD, изменения маршрутов и конфигураций могут приводить к дополнительным задержкам, поскольку сеть подстраивается под эти изменения. Эти изменения могут потребовать от пакетов прохождения более длинных и сложных маршрутов, что также приведет к увеличению задержек. Кроме того, смена одной конфигурации на другую также вносит значительные задержки, так как в эти периоды сеть адаптируется к новым параметрам.

Измерение задержек также необходимо для понимания влияния MTD на общую производительность передачи данных. MTD может привести к критическому снижению качества обслуживания, особенно для приложений, чувствительных к задержкам. Результаты измерений приведены в таблице 6.

Для оценки потери пакетов также использовался инструмент для тестирования пропускной способности сети iperf3. Значительных отклонений относительно результатов эксперимента без реконфигураций не наблюдается, а основные задержки возникали в результате переходов от одной конфигурации к другой.

Таблица 6 – Результаты измерений задержек между конфигурациями

Конфигурация									
№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	№ 7	№ 8	№ 9	№ 10
2 с	45 с	43 с	40 с	3 с	46 с	39 с	6 с	38 с	35 с
Конфигурация									
№ 11	№ 12	№ 13	№ 14	№ 15	№ 16	№ 17	№ 18	№ 19	№ 20
40 с	31 с	30 с	3 с	35 с	31 с	36 с	31 с	34 с	5 с

В результате перехода от одной реконфигурации к другой возникает задержка длительностью от 30 до 46 секунд, в среднем – 37 секунд, за исключением аномально коротких переходов.

3.3.8 Интерпретация результатов оценки на основе метрик

На основе полученных данных можно сделать следующие выводы:

1. Реализация предложенного алгоритма создает временные периоды, когда передача данных невозможна. Эти периоды возникают при смене одной топологии сетевого уровня на другую. 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.

2. Графики производительности сети (пропускная способность, задержки и потери пакетов) показывают то, что в то время, когда топология сетевого уровня уже развернута, предложенный алгоритм никак не влияет на производительность сети. Ухудшение производительности происходит именно из-за временных периодов, когда передача данных невозможна.

3. Чем чаще происходит смена топологии сетевого уровня, тем меньше информации о текущей топологии получит злоумышленник. Частота смены топологии никак не влияет на производительность передачи данных, но увеличивает частоту возникновения временных периодов, когда передача данных невозможна.

4. Аномально короткие временные периоды, когда передача данных невозможна, возникают по причине того, что хосты, на которых измерялась

производительность сети, оказывались в одной или в ближайших по количеству переходов группах. Фактически, новая топология сетевого уровня еще полностью не развернута, но между этими хостами уже есть обмен, а между двумя другими хостами, которые расположены друг от друга в нескольких переходах, обмена нет. Поэтому реальный период смены одной топологии сетевого уровня на другую составляет от 30 до 46 секунд.

5. Для того, чтобы улучшить производительность сети при использовании предложенного алгоритма, необходимо сокращать время 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, требуется значительное время. В дальнейшем по мере развития сетевого оборудования, ситуация может измениться. Во время того, когда смена топологии сетевого уровня уже произошла и сеть начала функционировать, предложенные метод, алгоритм и программное средство не вносят значительных накладных расходов.

6. Текущая реализация метода и алгоритма может быть применима для ИС нечувствительным к задержкам, то есть в тех, где не требуется обработки в режиме реального времени, не требуется мгновенного ответа и данные могут быть обработаны постфактум, например: системы мониторинга и сбора данных, системы управления дискретными процессами и так далее.

3.3.9 Оценка окна атаки

Окно атаки – это непрерывный период времени, который злоумышленник может использовать, не прерываясь из-за изменений поверхности атаки. Оценка окна атаки имеет важное значение для оптимизации MTD и создания баланса между повышением уровня ИБ и снижением производительности. 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 осу-

ществления действий, что потенциально может привести к успешной атаке до того, как произойдет следующая реконфигурация.

Оценка окна атаки важна, поскольку она показывает необходимые время и частоту изменений MTD. Окно атаки должно быть достаточно длинным, чтобы избежать чрезмерных сбоев в работе ИС, но достаточно коротким, чтобы злоумышленник не успел осуществить атаку. Эффективность MTD во многом зависит от того, насколько хорошо управляется окно атаки. Правильно выверенное окно атаки минимизирует вероятность успешных атак за счет сокращения времени на разведку, эксплуатацию уязвимости и выполнение атаки. Например, если злоумышленник находится в процессе эксплуатации уязвимости, но конфигурация ИС меняется до того, как он успевает завершить атаку, то, скорее всего, атака не удастся, и злоумышленник будет вынужден начать все сначала с новыми попытками разведки. Если окно атаки слишком длинное, это увеличивает риск того, что злоумышленник сможет воспользоваться уязвимостью и закрепиться в ИС. Этот риск особенно высок для современных APT-атак, которые характеризуются скрытностью и устойчивостью.

Хотя сокращение окна атаки может повысить уровень ИБ, оно также накладывает дополнительные требования на системные ресурсы. Частые изменения сети и путей маршрутизации могут привести к увеличению накладных расходов, потенциальным сбоям в легитимной работе ИС и увеличению потребления полосы пропускания. Этот компромисс между ИБ и производительностью ИС является критически важным моментом при внедрении MTD. Оценивая окно атаки, защитники должны принимать обоснованные решения об оптимальной частоте изменений. В средах с высокими требованиями ИБ более короткие окна атаки могут быть оправданы, несмотря на значительное негативное влияние на производительность передачи данных. Результаты оценки окна атаки приведены в таблице 7.

В таблице указан результат завершения сканирования (в процентах), длительность сканирования (в секундах), количество обнаруженных хостов

(от 1 до 12) и факт обнаружения целевого хоста (да/нет). Так как утилита выдает процент завершения не в режиме реального времени, а само сканирование запускалось вручную сразу после того, как сеть становится доступной, значения приведены с погрешностью. В качестве целевого выбран один случайный хост, который для всех конфигураций был одним и тем же.

В соответствии с документацией к используемой для эксперимента утилитой nmap, сканирование одного адреса, даже если на нем нет хоста, составит 600 мс [134]. Таким образом, чтобы просканировать все адресное пространство метода, потребуется приблизительно 65536×600 мс, что значительно превышает длительность испытания, поэтому необходимо скорректировать параметры эксперимента.

Таблица 7 – Результаты измерения окна атаки

Конфигурация				
№ 1	№ 2	№ 3	№ 4	№ 5
90 %; 398 с; 12; да.	82 %; 355 с; 12; да.	10 %; 37 с; 1; нет.	57 %; 260 с; 6; нет.	73 %; 297 с; 9; да.
Конфигурация				
№ 6	№ 7	№ 8	№ 9	№ 10
58 %; 254 с; 8; да.	59 %; 261 с; 4; да.	44 %; 194 с; 4; нет.	35 %; 162 с; 3; нет.	36 %; 165 с; 4; да.
Конфигурация				
№ 11	№ 12	№ 13	№ 14	№ 15
11 %; 45 с; 1; нет.	16 %; 69 с; 1; нет.	16 %; 70 с; 1; нет.	24 %; 97 с; 6; да.	15 %; 65 с; 1; нет.
Конфигурация				
№ 16	№ 17	№ 18	№ 19	№ 20
17 %; 69 с; 1; нет.	15 %; 64 с; 1; нет.	13 %; 61 с; 1; нет.	14 %; 64 с; 3; да.	23 %; 95 с; 1; нет.

Так как адресное пространство большое, злоумышленник не успеет исследовать его за 15 минут (900 секунд). И поэтому адресное пространство необходимо ограничить 20 подсетями с маской 24, в которых могут быть размещены группы. Доступное адресное пространство известно злоумышленни-

ку. Экспериментальным путем установлено, что злоумышленник успевает просканировать такую сеть приблизительно за 6 минут 42 секунд (402 секунд), что приблизительно равно критичному периоду реконфигурации в соответствии с разделом 2.3.3.

Команда для сканирования: *nmap -T5 -A -v -F -n --max-rtt-timeout=100ms --max-retries=1 <подсети для размещения групп>*.

Испытания проводились на каждой реконфигурации сети в соответствии с экспериментом, описанным в разделе 3.2.1, и дополнительно проведено два предварительных испытания:

1. без реагирования (объем полученной информации: 100 %, информация о целевом хосте получена: да, завершено за 402 секунды);

2. по обнаружению (объем полученной информации: < 1 %, информация о целевом хосте получена: нет).

Использовалась наиболее интенсивная стратегия сканирования – безумная стратегия с обнаружением хостов, определением ОС и версий, сканированием часто используемых портов, без разрешения имен. Для каждой конфигурации указано в процентах отношение объема полученной информации ко всему объему, доступному в рамках выбранной стратегии сканирования, и факт получение информации о целевом хосте. Некоторые из конфигураций были ограничены не только периодом реконфигурации, но и длительностью самого испытания (конфигурации № 3 и № 11).

Таким образом, на основе экспериментальных данных можно построить графики зависимости вероятности идентификации целевого хоста от времени сканирования. Предполагается, что злоумышленник идентифицирует хост как целевой только после завершения сканирования, т.е. когда определит все хосты сети. На рисунках 30-33 показаны графики в зависимости от периода реконфигурации относительно эксперимента без реконфигурации сети.

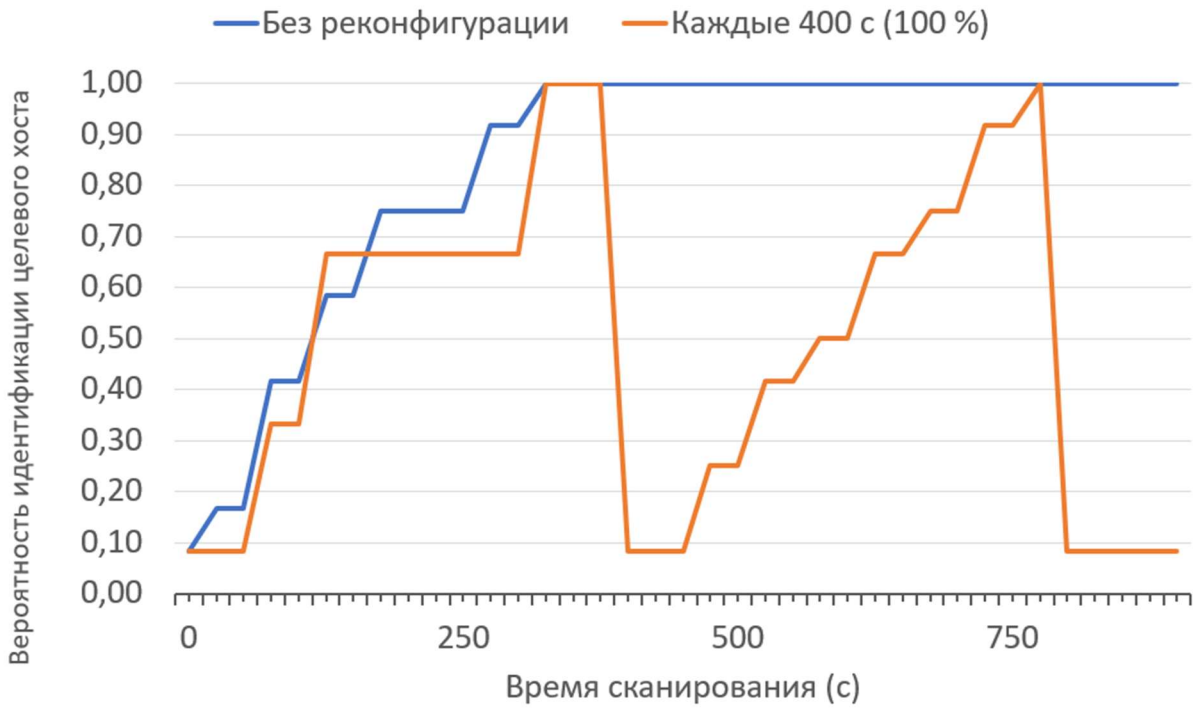

Рисунок 30 – График зависимости вероятности идентификации целевого хоста с реконфигурацией сети каждые 400 секунд

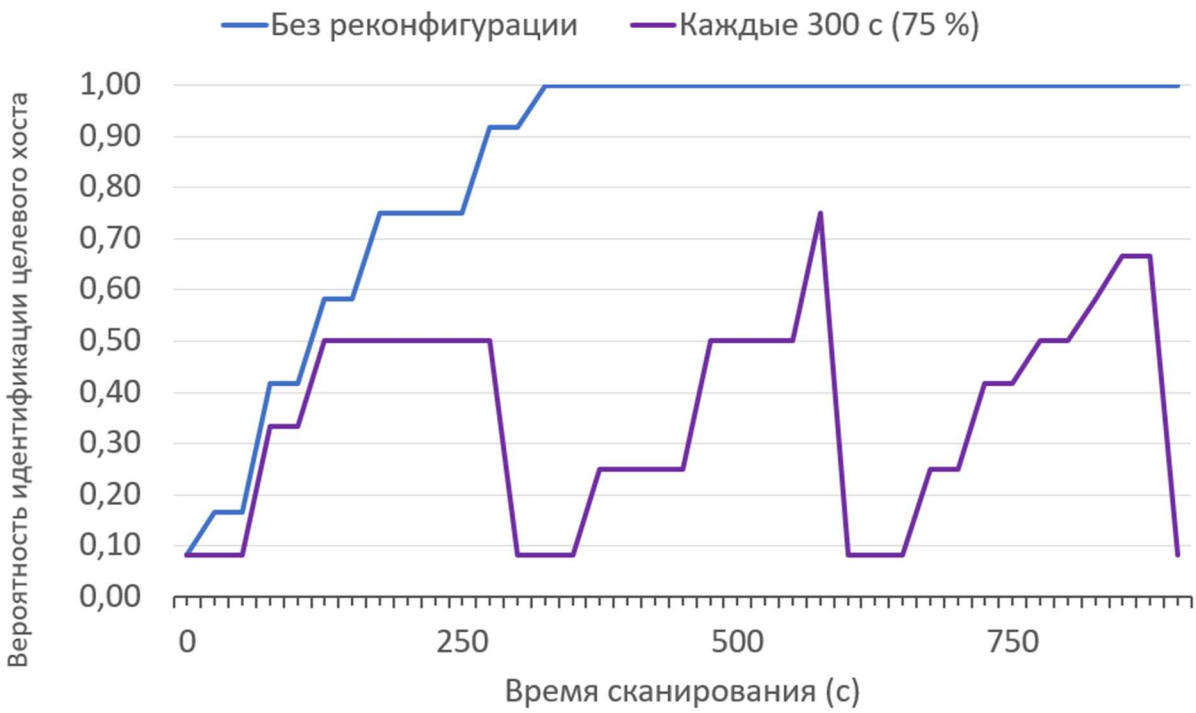

Рисунок 31 – График зависимости вероятности идентификации целевого хоста с реконфигурацией сети каждые 300 секунд

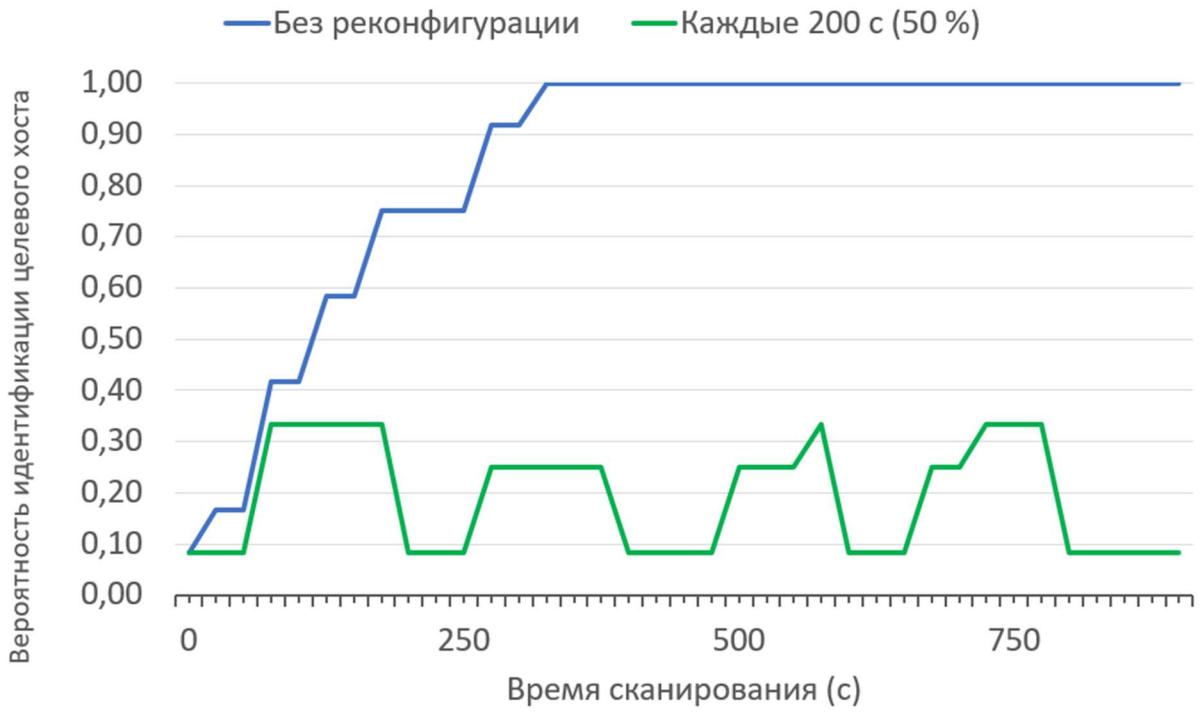

Рисунок 32 – График зависимости вероятности идентификации целевого хоста с реконфигурацией сети каждые 200 секунд

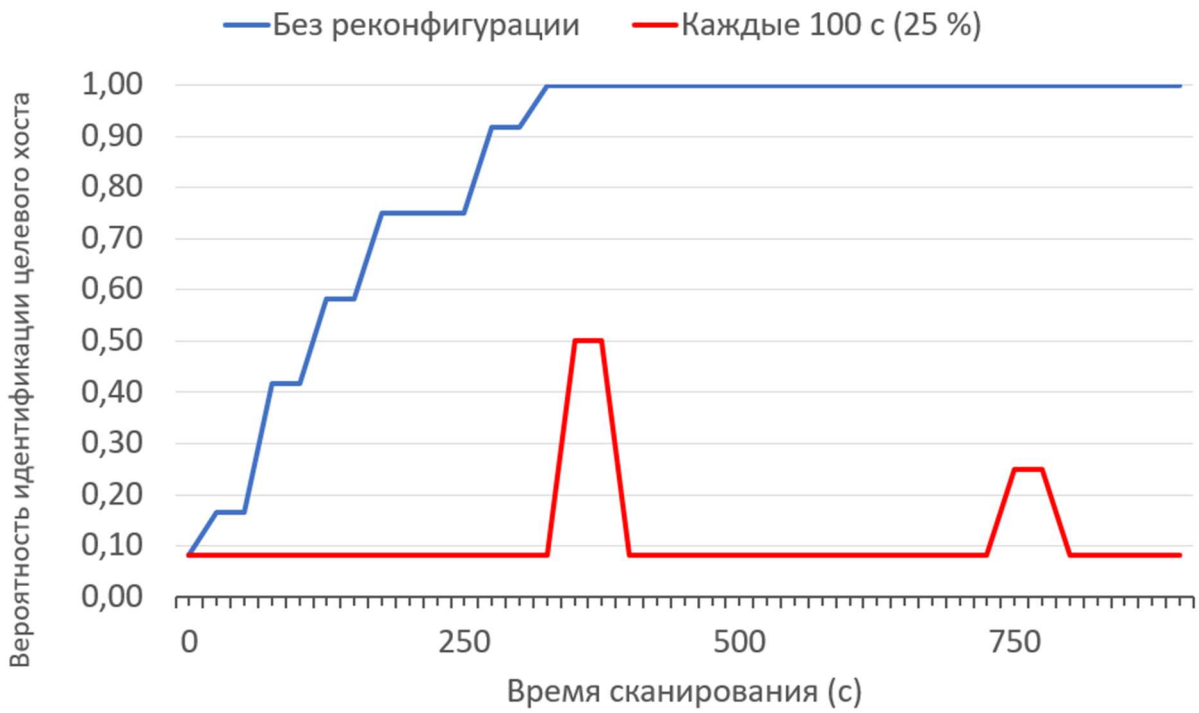

Рисунок 33 – График зависимости вероятности идентификации целевого хоста с реконфигурацией сети каждые 100 секунд

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.

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, которым завладел 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 алгоритм 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.

Также исходя из графиков можно предположить о том, что динамический случайный период даст более лучшие результаты по сравнению со статическим, так как в случае статического периода злоумышленник может проанализировать длительность каждой топологии сетевого уровня. Однако, в случае если период реконфигурации будет случайным образом выбран больше, чем критичный период, то злоумышленник успеет полностью исследовать сеть и перейти на следующую стадию реализации атаки. Кроме того, переход от одной топологии сетевого уровня к другой создает временной период, когда передача данных невозможна. Случайный выбор периода реконфи-

гурации может привести к тому, что сеть не будет функционировать из-за частой смены топологии сетевого уровня.

Поэтому выбор случайном величины периода реконфигурации будет происходить на узком числовом интервале, что не даст значительного повышения эффективности, так как злоумышленник также сможет при помощи анализа установить среднюю длительность периода, хотя и времени для этого ему потребуется несколько больше. Так как настоящая работа посвящена защите от стороннего исследования, то переход злоумышленника на следующую стадию реализации атаки является критичным. В случае, если не стоит принципиальной задачи именно защиты от исследования и допускается переход злоумышленника на следующую стадию реализации атаки, то интервал возможных случайных значений периода реконфигурации становится значительно шире, что, возможно, даст повышение эффективности.

3.4 Анализ полученных результатов оценки эффективности

Сравнение решений MTD имеет значение для выбора наиболее эффективного подхода к защите сети от исследования злоумышленником. Решения MTD различаются по производительности и эффективности противодействия.

3.4.1 Выбор существующих решений для сравнения

Для сравнения с существующими решениями были выбраны следующие работы [92, 116, 117, 130]. 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.

В работе [92] приведена реализация MTD, которая называется MT6D, выполненная на основе технологии IPv6. Эта реализация заключается в периодических изменениях адреса источника и назначения сетевого и транспортного уровней для взаимодействующих хостов. На каждом временном интервале MT6D вычисляет следующие IID (идентификатор интерфейса IPv6, ко-

торый может идентифицировать конкретный хост) для отправителя и получателя каждого сеанса взаимодействия, используя хэш-функцию и три параметра: текущий IID, общий симметричный ключ и системную метку времени. Таким образом, обе стороны взаимодействия могут вычислить IID. Временные интервалы различны для каждой пары взаимодействия, что оказывает положительное влияние на ИБ.

MT6D прозрачна для пользователя и не оказывает негативного влияния на взаимодействие, поскольку изменение адресов может быть произведено в середине текущей сессии без разрыва соединения или необходимости нового рукопожатия. Это является ключевой особенностью данного решения и это может увеличить трудозатраты на атаку для злоумышленника, поскольку адресное пространство IPv6 достаточно велико, а сеансы взаимодействия постоянно меняются. Однако системы MT6D должны поддерживать несколько IPv6-адресов для каждого хоста в любой момент времени, что приводит к дополнительным затратам.

В работе [116] приведена реализация MTD, которая 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, DNS-сервер оповещает SDN-контроллер. Затем SDN-контроллер генерирует синтетический IP-адрес и MAC-адрес для запрашиваемого сервера, устанавливает короткое значение TTL и отправляет их на DNS-сервер для ответа клиенту. SDN-контроллер отправляет команду серверу на установку правил трансляции сетевых адресов (NAT), которые преобразуют синтетические IP-адреса и MAC-адреса в реальные адреса. Таким образом, каждый клиент получает синтетические адреса сервера, которые могут быть изменены SDN-контроллером для каждого нового разрешения DNS.

В результате SDN-контроллер предоставляет изменяемые адреса для каждого клиента. А короткий TTL гарантирует, что клиент будет повторно

отправлять DNS-запросы для новых подключений, что позволяет серверу снова изменить адреса. SDN-контроллер конфигурирует сеть таким образом, чтобы сервер мог быть достижим по фиктивным адресам в рамках взаимодействия с ним. В результате сервер защищен от исследования, так как клиенту неизвестны настоящие адреса сервера, а использование недействительных адресов указывает на возможное исследование сети злоумышленником. Однако для реализации такого решения необходимо модифицировать DNS-сервер так, чтобы он имел возможность взаимодействовать с SDN-контроллером.

В работе [117] приведена реализация MTD, которая называется RPAH. Эта реализация основана на подходе случайного перехода по портам и адресам. Каждый серверный хост ассоциируется с неиспользуемым адресным пространством серверного домена (Virtual Address Range), а каждое приложение, работающее на серверном узле, ассоциируется с виртуальным диапазоном портов (Virtual Port Range), который представляет собой неиспользуемое пространство номеров портов узла. Через фиксированный интервал времени сервер изменяет свои IP-адреса и порты на основе псевдослучайной функции с общими секретными ключами, идентификатором источника, идентификатором сервиса и временем. Таким образом, клиенты должны использовать различные пары виртуальных адресов и номеров портов для получения услуг в разные временные интервалы, что может эффективно препятствовать исследованию злоумышленником.

RPAH должен модифицировать шлюзы, чтобы обеспечить механизм перехода адреса (Address Hopping Gateway), механизм перехода порта (Port Hopping Gateway), механизм одновременного перехода адреса и порта (Port and Address Hopping Gateway) для трансляций реального IP в виртуальный и обратно, реальный номер порта в виртуальный и обратно, а также пару из адреса и номера порта в виртуальную пару и обратно. В дополнение к затратам на модификацию, это влечет за собой большие накладные расходы на трансляцию, хранение, обновление и поиск информации об адресах. Однако такая

схема адресов и портов позволяет обнаружить злоумышленников, которые будут обращаться к серверам по недействительным адресам и портам.

В работе [130] 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.

В результате злоумышленник не может собрать необходимую информацию для манипулирования потоком данных. Главным преимуществом данного решения является отсутствие передачи управляющей информации, так как необходимые параметры вычисляются каждым узлом без передачи по каналам связи.

3.4.2 Сравнение с существующими решениями по характеристикам

Результаты сравнения предложенного метода с существующими решениями по характеристикам представлена в таблице 8.

Большинство существующих решений придерживаются генерации пространства конфигураций «на лету» и централизованной схемы управления [96], кроме [130].

Одним из главных преимуществ предложенного метода является возможность изоляции злоумышленника в случае его обнаружения. В тоже время большинство методов [92, 96, 116, 117, 130] сконцентрированы на том, чтобы заставить вести себя злоумышленника так, чтобы он выдал себя, например, обращаясь по устаревшим адресам.

Таблица 8 – Сравнение с существующими решениями по характеристикам

Характеристика	Предлагаемый метод	Dunlop M. (et al.) [92]	MacFarland D. C. (et.al) [116]	Luo Y. (et al.) [117]	Luo Y. (et al.) [130]
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.

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 [92, 96, 116, 117, 130] сконцентрированы на сокрытии реальных логических и физических адресов узлов 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.

3.4.3 Сравнение с существующими решениями по метрикам

Сводная таблица с результатами сравнения предложенного метода по метрикам с существующими решениями представлена в таблице 9.

Таблица 9 – Сравнение с существующими решениями по метрикам

Метрика	Предлагаемый метод	Dunlop M. (et al.) [92]	MacFarland D. C. (et.al) [116]	Luo Y. (et al.) [117]	Luo Y. (et al.) [130]
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

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.

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.

Накладные расходы адресного пространства не приводятся авторами работ в их публикациях. Нагрузка на сетевое оборудование также не оценена авторами работ, но исходя из того, как работают их решения, можно предположить, что нагрузка на сетевое оборудование должна быть в пределах общепринятых допустимых значений. Нагрузка на сетевое оборудование, создаваемая предложенным алгоритмом, также находится в пределах допустимых значений, при которых не возникает отказа в обслуживании и остается запас для других нагрузок.

3.4.3 Сравнение с другими решениями, влияющими на процесс исследования злоумышленником сети

Помимо ИО и MTD для противодействия исследования злоумышленником локальной сети передачи данных могут применяться и другие технологии. К ним можно отнести: виртуальные частные сети (Virtual Private Network, VPN), многопротокольная коммутация по меткам (MultiProtocol Label Switching, MPLS), брокеры сетевых пакетов (Network Packet Broker, NPB) и сетевая стеганография (стегоканал).

Технология VPN широко используется для повышения безопасности и конфиденциальности локальных сетей передачи данных. Шифруя передачу данных и скрывая топологию сети, VPN существенно влияют на способность

злоумышленника исследовать атакуемые ИС. VPN поддерживает частную сеть поверх публичной сети, позволяя пользователям отправлять и получать данные так, как если бы их устройства были напрямую подключены к частной сети. VPN используют протоколы шифрования, аутентификации и туннелирования для защиты данных.

VPN маскируют внутреннюю структуру сети, представляя внешним наблюдателям единственную точку входа. Злоумышленник, пытающийся составить карту сети с помощью внешнего сканирования, сталкивается с серьезными проблемами [120]:

1. VPN-шлюзы ограничивают видимость внутренних IP-адресов и сетевых устройств;

2. внешние клиенты не имеют прямого доступа к внутренним службам и не видны посторонним, что не позволяет злоумышленнику выявить потенциальные цели.

VPN в первую очередь защищает ИС от внешнего злоумышленника, поэтому эта технология неэффективна против внутреннего злоумышленника. Злоумышленник, имеющий учетные данные для доступа к ИС через VPN, никак не ограничен в исследовании. Злоумышленник может скомпрометировать устройства, которые имеют подключение к VPN. Технологии шифрования и туннелирования VPN оказывают негативное влияние на задержки, накладные расходы на передачу и пропускную способность [120].

Технология MPLS – это технология передачи данных для высокопроизводительных телекоммуникационных сетей, которая направляет данные от одного узла сети к другому на основе коротких меток пути, а не длинных сетевых адресов, таким образом избегая сложных поисков маршрутов в таблице маршрутизации. Основные особенности данной технологии:

1. коммутация меток, то есть решения о пересылке принимаются на основе меток, которыми помечены все пакеты;

2. перераспределение трафика, то есть MPLS поддерживает механизмы организации трафика, при помощи которых она может оптимизировать использование сетевых ресурсов;

3. управление качеством обслуживания, что достигается за счет классификации и управления сетевым трафиком;

4. масштабируемость.

Технология MPLS предназначена для повышения производительности сетей за счет маршрутизации на основе меток. Использование меток при маршрутизации оказывает побочное влияние на исследование злоумышленником локальной сети передачи данных. MPLS использует метки для принятия решений о пересылке, которые не раскрываются внешним субъектам. Это скрывает топологию сети от исследования злоумышленником. Использование меток, скрывает схемы IP-адресации, что затрудняет злоумышленнику точное картирование сети. Также MPLS инкапсулирует пакеты с метками, что усложняет работу по перехвату и анализу сетевых пакетов. Метки меняются при каждом переходе, что не позволяет злоумышленнику отслеживать пакеты в сети при помощи значений меток. Однако, злоумышленник может манипулировать метками для перенаправления трафика [121].

NPB – это аппаратное или программное решение, которое располагается между сетевыми устройствами и средствами мониторинга/ИБ. NPB агрегирует трафик с нескольких сетевых каналов и интеллектуально перенаправляет определенные потоки данных соответствующим инструментам ИБ на основе заранее определенных политик. NPB является важным компонентом современной сетевой инфраструктуры, способствуя эффективному управлению трафиком, мониторингу и обеспечению ИБ. Агрегируя, фильтруя и распределяя сетевой трафик, NPB улучшает видимость и контроль над потоками данных в локальных сетях передачи данных. NPB обеспечивает централизованную платформу для обработки сетевого трафика, позволяя эффективно передавать данные различным службам и сервисам ИБ, развернутых в сети.

Основные функции NPB [122]:

1. агрегация, то есть объединение сетевого трафика от различных источников для всестороннего анализа;

2. фильтрация и переадресация, то есть блокирование, ограничение скорости, выборочное перенаправление на конкретные средства мониторинга/ИБ определенного сетевого трафика;

3. балансировка нагрузки, то есть перераспределение трафика между несколькими инструментами для снижения нагрузки на каждый конкретный инструмент;

4. дедупликация, то есть устранение избыточных пакетов;

5. модификация пакетов, то есть маскирование конфиденциальной информации или извлечение избыточной информации, в том числе из заголовков пакетов в соответствии с требованиями ИБ.

Прямое назначение NPB это управление трафиком и его перераспределение. Как правило, NPB применяют для эффективного мониторинга и обнаружения вторжений в режиме реального времени. Однако, побочным действием управления трафиком является ограничение области видимости для злоумышленника при исследовании локальной сети передачи данных. Применение NPB может оказывать негативное влияние на пропускную способность и на задержки, так как требуется обработка пакетов в режиме реального времени [122].

Сетевая стеганография включает в себя скрытое встраивание информации в сетевой трафик для сокрытия обмена данными или схем сетевого взаимодействия. Традиционно сетевая стеганография ассоциируется с организацией скрытых каналов связи злоумышленником, однако она может также использоваться в качестве защитного механизма для противодействия исследованию злоумышленником локальной сети передачи данных.

Методы сетевой стеганографии направлены на модификацию данных в заголовках и полях полезной нагрузки сетевых пакетов и на изменение структуры передачи пакетов. Обычно данные просто скрываются в элементах управления протоколов связи и в простых пакетах данных, но также может

изменяться очередность передачи пакетов или могут преднамеренно теряться пакеты при их передаче. Скрытая передача осуществляется без изменения самой информации и без нарушений функциональности сетевых сервисов и служб. Однако технология сетевой стеганографии сложна во внедрении, управлении и применении, имеет существенные ограничения на объем передаваемой информации и низкую производительность передачи данных [123].

Для сравнения предложенного метода с существующими решениями, которые оказывают влияние на процесс исследования злоумышленником локальной сети передачи данных, необходимо выделить ряд общих метрик и характеристик, по которым они могут быть сравнены. На основании работ [96, 120, 121, 122, 123] выделены следующие характеристики для сравнения:

1. схема управления;
2. влияние на производительность передачи данных;
3. влияние на стабильность работы всей сети;
4. изменение правил управления каналом в режиме реального времени;
5. сокрытие данных сеансов связи;
6. сокрытие метаданных сеансов связи.

Схема управления аналогична характеристике из сравнения с существующими решениями MTD. Централизованное управление создает единую точку отказа всей системы, в отличие от частично централизованных и децентрализованных схем.

Среди выбранных технологий по данной характеристике отличаются:

1. стегоканал, так как является децентрализованным решением;
2. технология MPLS, так как является частично централизованным решением.

Влияние на производительность передачи данных и на стабильность работы всей сети определяет применимость технологии. Среди перечисленных технологий выгодно отличается MPLS, так как назначение этой технологии как раз и заключается в повышении производительности передачи данных и улучшении стабильности работы сети.

Технология NPB влияет на производительность передачи данных негативным образом, так как обрабатывает сетевой трафик в режиме реального времени, однако степень влияния на производительность остается приемлемой во всех случаях. При этом NPB улучшает стабильность всей сети благодаря фильтрации, переадресации, балансировке нагрузки и дедупликации.

VPN ухудшает производительность передачи данных на приемлемую величину только для клиента. На стабильность работы сети VPN никак не влияет.

Технология сетевой стеганографии является крайне непроизводительной с точки зрения передачи данных и может применяться только для небольшого объема данных.

Предложенный метод ухудшает производительность передачи данных и стабильной работы всей сети из-за смены топологии сетевого уровня на другую. Степень снижения производительности сети приемлема для ИС нечувствительным к задержкам.

Наличие возможностей изменения правил управления каналом в режиме реального времени указывает на потенциальную возможность технологии быть основой решения MTD. Потенциально для организации сети MTD могут быть применены технологии MPLS и NPB.

Сокрытие передаваемых данных и сокрытие метаданных сеансов связи влияет на исследование злоумышленником локальной сети передачи данных. В случае если данные и метаданные скрыты, злоумышленник не сможет получить и использовать эти данные в своих деструктивных целях.

Технология VPN осуществляет сокрытие данных и метаданных только от внешнего злоумышленника.

Технология MPLS благодаря меткам вносит неопределенность для злоумышленника в исследовании маршрутов передачи данных. При этом ничего не мешает использовать другие технологии сокрытия метаданных и шифрования данных совместно с MPLS.

Технология NPB также осуществляет частичное сокрытие метаданных путем дедупликации и модификации пакетов. NPB не препятствует использованию других технологий для сокрытия метаданных и самих данных.

Стегоканал осуществляет сокрытие факта передачи информации, а при совместном использовании с шифрованием могут быть скрыты и сами данные.

Предложенный метод не скрывает метаданные соединений: на каждой последующей конфигурации возникают новые соединения полностью отличные от предыдущих. Предложенный метод никак не ограничивает в использовании других технологий сокрытия данных и метаданных. Примененные при реализации предложенного алгоритма технологии позволяют такое совместное использование.

Результаты сравнения приведены в таблице 10.

Таблица 10 – Сравнение с другими решениями

№	VPN	MPLS	NPB	Стегоканал	Пр. метод
1	Центр.	Част. центр.	Центр.	Децентр.	Центр.
2	Ухудшает	Улучшает	Ухудшает	Ухудшает	Ухудшает
3	Не влияет	Улучшает	Улучшает	Не влияет	Ухудшает
4	Нет	Да	Да	Нет	Да
5	Да	Нет	Нет	Нет	Нет
6	Да	Частично	Частично	Да	Нет

Предложенный метод главным образом отличается от других рассмотренных решений своей ориентацией на противодействие исследованию злоумышленником локальной сети передачи данных, тогда как в других решениях это лишь побочных эффект. Соответственно, в других решениях сеть защищена от исследования лишь в некоторых аспектах, например, только от внешнего злоумышленника, от исследования маршрутов и так далее. Предложенный метод защищает сеть от исследования злоумышленником, который действует изнутри локальной сети передачи данных на любом из её хостов, при этом метод манипулирует более широким набором параметров.

3.5 Описание внедрений результатов диссертационной работы

Внедрение результатов работы показывает главным образом потенциальную применимость предложенного метода для решения реальных задач ИБ. Предложенный метод был внедрен в АО «НПП «Радиосвязь» и СибГУ им. М. Ф. Решетнева (приложение 3).

3.5.1 Применение предложенного метода для защиты от исследования злоумышленником на имитаторе станции связи АО «НПП «Радиосвязь»

В рамках своей коммерческой деятельности АО «НПП «Радиосвязь» разрабатывает станции связи. Для тестирования систем управления, а также апробации перспективных технологий и решений существует исследовательский стенд, который имитирует поведение типовой станции связи в соответствии с рисунком 34.

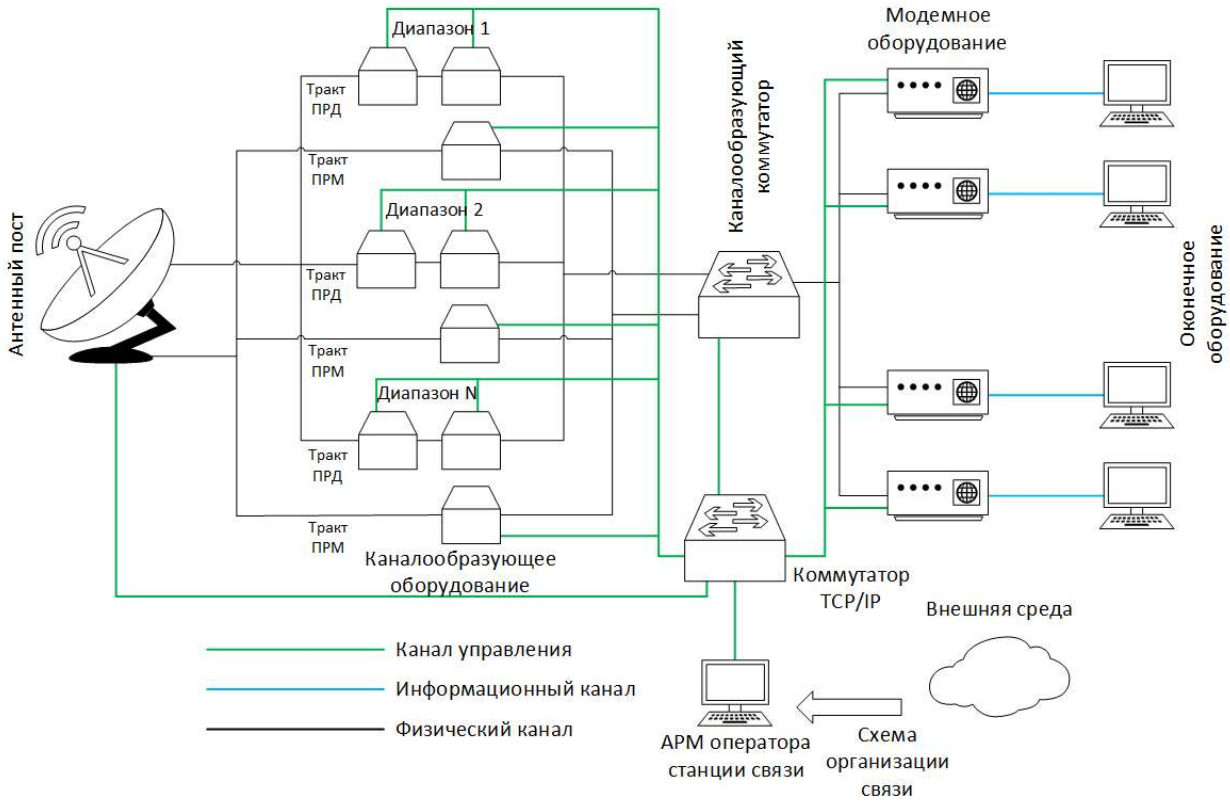

Рисунок 34 – Типовая схема станции связи

Управление станцией связи осуществляется по каналу управления, который представляет из себя Ethernet локальную вычислительную сеть стека TCP/IP с топологией типа «звезда» или «дерево». Каждое оборудование станции имеет Ethernet-интерфейс управления, которые подключено к сетевому оборудованию. Задача управления в станции связи заключается в задании такого режима работы каналообразующего и модемного оборудования, чтобы это оборудование работало между собой согласованно и в соответствии с заданной схемой организации связи. Схема организации связи, топология и состав оборудования станции являются информацией ограниченного доступа, поэтому существует необходимость защиты станции от исследования злоумышленником.

Исследовательский стенд был развернут в виртуальной среде EVE-NG, где некоторые отдельные хосты представляют собой виртуальную машину на базе ОС Ubuntu 22.04, ПО на котором имитирует определенное устройство в составе станции (далее – имитатор): принимает управляющие команды, имитирует различные состояния и так далее. Одним из хостов сети управления является автоматизированное рабочее место (АРМ) оператора станции связи, которое функционирует под управлением ОС Ubuntu 22.04 и на нем развернуто ПО управления (далее – подсистема автоматизированного управления, ПАУ) станицей связи. Все хосты (ПАУ и имитаторы) объединены в единую сеть с топологией типа «звезда» на базе коммутатора под управлением ОС NX-OS. Обмен информацией между хостами в сети управления осуществляется по протоколу UDP, прикладные данные пакетов которого кодируются в соответствии с протоколами на устройства.

При внедрении предложенного алгоритма и реализующего его программного средства была поставлена цель по анализу потенциальной применимости технологий MTD для решения прикладной задачи по защите от исследования злоумышленником канала управления. Имитаторы и ПАУ разработаны таким образом, чтобы пользователи могли влиять на чувствительность к задержкам при помощи управления различными параметрами. Кроме

того, ПАУ и имитаторы можно модифицировать в соответствии с необходимостью по внедрению предложенного метода.

В результате анализа были получены следующие результаты: вносимое предложенным методом снижение производительности передачи данных приемлемо для некоторых схем организации связи. Однако, существуют схемы, для которых критичны задержки и потери пакетов, и они не могут функционировать в такой среде. Это связано с несколькими факторами.

Во-первых, устройства передают ПАУ некоторые данные о своем состоянии, которые требуют обработки. После их обработки ПАУ непрерывно и оперативно корректирует режим работы в соответствии с данными состояния.

Во-вторых, по каналам управления передаются не только управляющие команды ПАУ и ответы устройств, но и сами устройства обменивается между собой данными, которые требуют оперативного реагирования.

3.5.2 Внедрение результатов работы в образовательный процесс СибГУ

Результаты диссертационной работы были внедрены в образовательный процесс для студентов кафедры безопасности информационных технологий СибГУ им. М. Ф. Решетнева в рамках модуля «Технологии информационного обмана и защиты с использованием подвижных целей» курсов «Сети и системы передачи информации» и «Безопасность облачных технологий». Программное средство, реализующее предложенный алгоритм, позволяет на практике познакомить студентов со способами исследования локальных сетей передачи данных, а также современными подходами по противодействию их исследованию злоумышленником.

При помощи программного средства можно создать сеть MTD и предпринимать попытки исследовать её. Сравнение попыток исследовать статичную сеть и сеть MTD демонстрирует студентам механизмы MTD и их влияние на процесс исследования сети злоумышленником.

Также предложенный метод, математическая модель, алгоритм, программное средство и результаты оценки эффективности используются в их

собственных научно-исследовательских проектах, направленных на построение активной системы ЗИ.

Комплект практических заданий, разработанный на основе выполненной работы, включает (помимо методических материалов):

1. Скрипт по автоматизированной настройке окружения ОС Ubuntu 22.04.

2. Скрипт по автоматизированной настройке сетевого оборудования на базе ОС NX-OS.

3. Скрипт по распространению ПО предложенного метода по инфраструктуре.

4. Исходный код предложенного метода.

Данный набор позволяет сконцентрироваться именно на аспектах технологии MTD и избежать ошибок при развертывании тестового стенда, а также он позволяет реализовать свои идеи по улучшению предложенного метода.

3.6 Выводы

1. В данной главе был проведен анализ эффективности предложенного метода. 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.

2. 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 параметры 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.

3. 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.

4. Была проведена оценка окна атаки для предложенного метода. Предложенный метод сокращает окно атаки для злоумышленника, изменяя поверхность атаки, на величину, которая зависит от выбранного периода. После

каждой реконфигурации, оценка вероятности идентификации целевого хоста составила $1/N$, где N – это количество хостов сети. Данная оценка получена эмпирически.

5. 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.

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

7. 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.

ЗАКЛЮЧЕНИЕ

Основные результаты и выводы, полученные в ходе проведения исследования, заключаются в следующем:

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, длитель-

ностью 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 анализа 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.

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.

СПИСОК СОКРАЩЕНИЙ

API – Application Programming Interface

ARP – Address Resolution Protocol

DDP – Deception Disturbed Platform

DiD – Defense-in-Depth

DNS – Domain Name System

EDR – Endpoint Detection and Response

HTTP – HyperText Transfer Protocol

ICMP – Internet Control Message Protocol

ID – Identificator

IDPS – Intrusion Detection and Prevention Systems

IEEE – the Institute of Electrical and Electronics Engineers

IoT – Internet of Things

IP – Internet Protocol

JSON – JavaScript Object Notation

JSON RPC – JSON Remote Procedure Call

MAC – Media Access Control

MITM – Man-In-The-Middle

MPLS – MultiProtocol Label Switching

MTD – Moving Target Defense

NAT – Network Address Translation

NPB – Network Packet Broker

SDN – Software Defined Network

SIEM – Security Information and Event Management

SOAR – Security Orchestration, Automation and Response

SSL – Secure Sockets Layer

TCP – Transmission Control Protocol

TIP – Threat Intelligence Platforms

TTL – Time-To-Live

UDP – User Datagram Protocol

VLAN – Virtual Local Area Network

VNI – VXLAN Network Identificator

VPN – Virtual Private Network

VXLAN – Virtual eXtensible Local Area Network

YAML – YAML Ain't Markup Language

ZTA – Zero Trust Architecture

АРМ – Автоматизированное рабочее место

БД – База данных

ЗИ – Защита информации

ИБ – Информационная безопасность

ИО – Информационный обман

ИС – Информационная система

МЭ – Межсетевой экран

ОС – Операционная система

ПАУ – Подсистема автоматизированного управления

ПК – Персональный компьютер

ПЛИС – Программируемая логическая интегральная схема

САВЗ – Средство антивирусной защиты

СЗИ – Средство защиты информации

СОВ – Средство обнаружения вторжений

СУБД – Система управления базами данных

СЛОВАРЬ ТЕРМИНОВ

Deception: технология информационного обмана, категория систем управления ложными объектами.

Moving Target Defense: технология защиты с использованием подвижных целей, технология управления изменениями качеств и поведения системы с целью повышения неопределенности и кажущейся сложности для атакующих, уменьшая возможности и увеличивая затраты на их зондирование и атаку.

Группа участников взаимодействия: выделенный в единую подсеть набор участников взаимодействия.

Защищенность локальной сети передачи данных от стороннего исследования: вероятность идентификации целевого хоста.

Критичный период реконфигурации: время, которое необходимо злоумышленнику для сбора информации о сети и последующего перехода к следующей стадии реализации атаки, по его истечению топология сетевого уровня должна быть реконфигурирована.

Локальная сеть передачи данных: локальная сеть, предназначенная для обмена данными между устройствами (в том числе и не вычислительными: датчики, камеры, контроллеры и т.п.) с использованием стандартных или специализированных протоколов, в то время как локальная вычислительная сеть – это частный случай локальной сети передачи данных, и она ориентирована на взаимодействие между вычислительными устройствами (компьютеры, серверы и т.п.).

Окно атаки: непрерывный период времени, который злоумышленник может использовать, не прерываясь из-за изменений поверхности атаки.

Поверхность атаки: 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.

Подвижная цель: это динамически и периодически изменяемый объект сети или ИС для того, чтобы затруднить злоумышленнику исследование сети.

Потенциально опасный хост: хост сети MTD, который, возможно, осуществляет исследование сети.

Правила исключения: правила, в соответствии с которыми осуществляется исключение потенциально опасных хостов.

Реконфигурация: смена текущей конфигурации на новую.

Сеть MTD: сегмент локальной сети передачи данных, в котором функционирует технология Moving Target Defense.

Топология сетевого уровня: набор параметров сети, который включает в себя: физический и логический адреса, маршруты передачи данных и логическую топологию сети.

Участник взаимодействия: один из множества взаимодействующих друг с другом хостов сети MTD.

Участник-клиент: участник взаимодействия, который не управляет сетью. Этот хост лишь принимает конфигурации и применяет их, а также оповещает участника-сервера о наступлении некоторых событий.

Участник-сервер: участник взаимодействия, на которого возложена роль контроллера сети MTD, то есть он реконфигурирует топологию сетевого уровня, а именно по наступлению определенных событий формирует пространство конфигураций и рассылает их участникам взаимодействия и сетевому оборудованию.

Участник-шлюз: участник взаимодействия, который был выбран в качестве шлюза и является внутренним/внешним по отношению к группе, то есть он изначально был (внутренний)/не был (внешний) её участником при формировании групп участников взаимодействия.

Физическое описание сети: описание физического и канального уровня сети MTD, которое включает в себя: список сетевого оборудования с указанием имен и логических адресов их интерфейсов; список хостов, с указанием их имен и адресов; описание физических подключений между хостами и се-

тевыми оборудованием, то есть: имя сетевого устройства, имя интерфейса, имя подключенного к нему хоста, имя сетевого адаптера хоста.

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.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Cyber Kill Chain [Электронный ресурс]. – URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 19.09.2024).

2. Rahman M. T. Defense-in-depth: A recipe for logic locking to prevail / M. T. Rahman, M. S. Rahman, S. Tajik [et al.] // Integration. – 2020. – V. 72. – P. 39-57.

3. Cleghorn, L. Network defense methodology: A comparison of defense in depth and defense in breadth // Journal of Information Security. – 2013. – V. 4., No. 3. – 6 p.

4. Rocha F. Defense-in-depth against malicious insiders in the cloud / F. Rocha , T. Gross, A. Van Moorsel // 2013 IEEE International Conference on Cloud Engineering (IC2E). – IEEE, 2013. – P. 88-97.

5. National Institute of Standards and Technology. NIST Special Publication 800-207. Zero Trust Architecture [Электронный ресурс]. – URL: https://csrc.nist.gov/pubs/sp/800/207/final (дата обращения: 19.09.2024)

6. Cao Y. Automation and orchestration of zero trust architecture: Potential solutions and challenges / Y. Cao, S. R. Pokhrel, Y. Zhu [et al.] // Machine Intelligence Research. – 2024. – V. 21, No. 2. – P. 294-317.

7. Mohammad S. M. Security automation in Information technology / S. M. Mohammad, L. Surya // International journal of creative research thoughts (IJCRT) – 2018. – V. 6, No. 2. – P. 901-905.

8. Strand J. Offensive Countermeasures: The Art of Active Defense / J. Strand, P. Asadoorian, E. Robish [et al.]. – CreateSpace Independent Publishing Platform, 2013. – 168 p.

9. Active Defense: Using Deception and Trickery to Defeat Cyber Adversaries [Электронный ресурс]. – URL: https://www.mitre.org/news-insights/impact-story/active-defense-using-deception-and-trickery-defeat-cyber-adversaries (дата обращения: 19.09.2024).

10. Nour B. A survey on threat hunting in enterprise networks / B. Nour, M. Pourzandi, M. Debbabi // IEEE Communications Surveys & Tutorials. – 2023. – V. 25. – P. 2299-2324.

11. Karlzen H., Sommestad T. Automatic incident response solutions: a review of proposed solutions' input and output / H. Karlzen, T. Sommestad // Proceedings of the 18th International Conference on Availability, Reliability and Security. – 2023. – P. 1-9.

12. Guerra L. M. F. C. Proactive Cybersecurity tailoring through deception techniques [Электронный ресурс]. – URL: https://repositorio.ipl.pt/bitstream/10400.21/16947/1/LuisGuerra_43755_MEIC.pdf (дата обращения: 19.09.2024).

13. Карвальо М. Защита сетей путем создания движущихся целей / М. Карвальо, Р. Форд // Открытые системы. – 2014. – № 4.

14. Sarker I. H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects // Annals of Data Science. – 2023. – V. 10, No. 6. – P. 1473-1498.

15. Rosenzweig P. Next steps for US cybersecurity in the trump administration: Active cyber defense / P. Rosenzweig, S. P. Bucci, D. Inserra // Backgrounder. – 2017. – V. 3188, No. 11.

16. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 [Электронный ресурс]. – URL: https://complexdiscovery.com/wp-content/uploads/2019/10/Framework-for-Improving-Critical-Infrastructure-Cybersecurity.pdf (дата обращения: 19.09.2024).

17. Debar H. Security Operations & Incident Management Knowledge Area Issue 1.0. – The Cyber Security Body of Knowledge, 2019. – 47 p.

18. Saint-Hilaire K. A. Optimal automated generation of playbooks / K. A. Saint-Hilaire, C. Neal, F. Cuppens [et al.] // IFIP Annual Conference on Data and Applications Security and Privacy. – 2024. – P. 191-199.

19. Varga S. Automation of Cybersecurity Work / S. Varga, T. Sommestad, J. Brynielsson // Artificial Intelligence and Cybersecurity: Theory and Applications. – 2022. – P. 67-101.

20. Huang Y. Reinforcement learning for feedback-enabled cyber resilience / Y. Huang, L. Huang, Q. Zhu // Annual reviews in control. – 2022. – V. 53. – P. 273-295.

21. Schlette D. Do you play it by the books? A study on incident response playbooks and influencing factors / D. Schlette, P. Empl, Caselli M. [et al.] // 2024 IEEE Symposium on Security and Privacy (SP). – 2024. – P. 3625-3643.

22. Virvilis N. Changing the game: The art of deceiving sophisticated attackers / N. Virvilis, B. Vanautgaerden, O. S. Serrano // 2014 6th International Conference On Cyber Conflict (CyCon 2014). – 2014. – P. 87-97.

23. Positive Technologies. Positive Research 2020 [Электронный ресурс]. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf (дата обращения: 19.09.2024).

24. Positive Technologies. Positive Research 2019 [Электронный ресурс]. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2019-rus.pdf (дата обращения: 19.09.2024).

25. Verizon. Results and Analysis: Introduction [Электронный ресурс]. – URL: https://ww.verizon.com/business/resources/reports/dbir/2023/results-and-analysis-intro/ (дата обращения: 19.09.2024).

26. Cyber Detection for Insider Threats: What You Need to Know [Электронный ресурс]. – URL: https://www.bankinfosecurity.com/whitepapers/cyber-detection-for-insider-threats-what-you-need-to-know-w-11180 (дата обращения: 19.09.2024).

27. McCargo H. Proactive vs. Reactive Cyber Security Compared – What's the Difference? [Электронный ресурс]. – URL: https://www.bankinfosecurity.com/whitepapers/cyber-detection-for-insider-threats-what-you-need-to-know-w-11180 (дата обращения: 19.09.2024).

28. Resilient X. Reactive vs. Proactive Security: A Comprehensive Guide to Enhancing Cybersecurity Effectiveness [Электронный ресурс]. – URL: https://resilientx.com/blog/reactive-vs-proactive-security-a-comprehensive-guide-to-enhancing-cybersecurity-effectiveness/ (дата обращения: 19.09.2024).

29. Методический документ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах» [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/675 (дата обращения: 19.09.2024).

30. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. – 2013. – № 107.

31. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 14 марта 2014 г. № 31 «Требования к обеспечению защиты информации в АСУ ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды» // Российская газета. – 2014. – № 175.

32. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. – 2013. – № 136.

33. Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // Российская газета. – 2018.

34. General Data Protection Regulation [Электронный ресурс]. – URL: https://gdpr-info.eu/ (дата обращения: 19.09.2024).

35. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200181890 (дата обращения: 19.09.2024).

36. ГОСТ Р ИСО/МЭК 27002-2021 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200179669 (дата обращения: 19.09.2024).

37. ГОСТ Р ИСО/МЭК 27033-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей» [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200089172 (дата обращения: 19.09.2024).

38. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 [Электронный ресурс]. – URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата обращения: 19.09.2024).

39. National Institute of Standards and Technology. NIST Special Publication 800-47 Revision 1. Managing the Security of Information Exchanges [Электронный ресурс]. – URL: https://csrc.nist.gov/pubs/sp/800/47/r1/final (дата обращения: 19.09.2024).

40. National Institute of Standards and Technology. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations [Электронный ресурс]. – URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата обращения: 19.09.2024).

41. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [Электронный ресурс]. – URL: http://cbr.ru/statichtml/file/59420/st-10-14.pdf (дата обращения: 19.09.2024).

42. Payment Card Industry Data Security Standard v4.0.1 [Электронный ресурс]. – URL: https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1 (дата обращения: 19.09.2024).

43. HIPAA Security Standards: Technical Safeguards [Электронный ресурс]. – URL: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (дата обращения: 19.09.2024).

44. Защита от сканирования портов — PSD в mikrotik [Электронный ресурс]. – URL: https://mikrotik-training.ru/kb/zashhita-ot-skanirovaniya-portov-psd-v-mikrotik/ (дата обращения: 19.09.2024).

45. РБК. Что такое сниффер и как не лишиться данных после покупок в интернете [Электронный ресурс]. – URL: https://trends.rbc.ru/trends/industry/60f6c2af9a7947fc32ae0a91 (дата обращения: 19.09.2024).

46. Varonis Systems. Man-in-the-Middle: советы по обнаружению и предотвращению [Электронный ресурс]. – URL: https://habr.com/ru/companies/varonis/articles/526632/ (дата обращения: 19.09.2024).

47. Baranowski R. Access port protection for reconfigurable scan networks / R. Baranowski, M. A. Kochte, H. J. Wunderlich // Journal of Electronic Testing. – 2014. – V. 30, No. 6. – P. 711-723.

48. Новиков И. Д. Защита информации от сетевого сниффинга внутри организации // Доклады Всероссийской конференции (с международным участием) «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (РЭУС-2022). – Москва, 2022. – С. 287-290.

49. Ali M. L. Network packet sniffing and defense / S. Ismat, K. Thakur, A. Kamruzzaman [et al.] // 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). – 2023. – P. 499-503.

50. Ростелеком Солар. Solar JSOC Security Report [Электронный ресурс]. – URL: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf (дата обращения: 19.09.2024).

51. Kaspersky ICS CERT. APT-атаки на промышленные компании в 2020 году [Электронный ресурс]. – URL: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-companies-in-2020-Ru.pdf (дата обращения: 19.09.2024).

52. Infowatch. Утечки данных. Россия. 2016 год [Электронный ресурс]. – URL: https://www.infowatch.ru/analytics/reports/17962 (дата обращения: 19.09.2024).

53. JSOC. JSOC Security flash report [Электронный ресурс]. – URL: https://www.anti-malware.ru/news/2015-07-09/16455 (дата обращения: 19.09.2024).

54. Перспективный мониторинг. Отчёт Центра мониторинга за второе полугодие 2017 года [Электронный ресурс]. – URL: https://amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2017-2_amonitoring_halfyear_report.pdf (дата обращения: 19.09.2024).

55. Перспективный мониторинг. Отчёт Центра мониторинга за первое полугодие 2018 года [Электронный ресурс]. – URL: https://amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2018-1_amonitoring_halfyear_report.pdf (дата обращения: 19.09.2024).

56. Ivanti. 2024 State of Cybersecurity Report [Электронный ресурс]. – URL: https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report (дата обращения: 19.09.2024).

57. Check Point. 2023 Cyber Security Report [Электронный ресурс]. – URL: https://www.checkpoint.com/downloads/resources/2023-cyber-security-report.pdf (дата обращения: 19.09.2024).

58. Sophos. Sophos 2024 Threat Report: Cybercrime on Main Street [Электронный ресурс]. – URL:

https://assets.sophos.com/X24WTUEQ/at/wwf5phjtj9bjvmpqqsbfxc/sophos-2024-threat-report.pdf (дата обращения: 19.09.2024).

59. Sirar. Threat Landscape Report in 2023 [Электронный ресурс]. – URL: https://www.sirar.com.sa/wp-content/uploads/2024/02/Threat-Landscape-Report-in-2023-Final.pdf (дата обращения: 19.09.2024).

60. Cyber Security Council. CPX. State of the UAE. Cybersecurity Report 2024 [Электронный ресурс]. – URL: https://www.cpx.net/media/hocl331j/state-of-the-uae-cybersecurity-report.pdf (дата обращения: 19.09.2024).

61. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023 [Электронный ресурс]. – URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата обращения: 19.09.2024).

62. MITRE. MITRE ATT&CK [Электронный ресурс]. – URL: https://attack.mitre.org/ (дата обращения: 19.09.2024).

63. Lackner P. How to Mock a Bear: Honeypot, Honeynet, Honeywall & Honeytoken: A Survey // ICEIS (2). – 2021. – P. 181-188.

64. Данилова Е. Обзор рынка платформ для создания распределенной инфраструктуры ложных целей (Distributed Deception Platform) [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/Distributed-Deception-Platform (дата обращения: 19.09.2024).

65. Mohan P. V. Leveraging computational intelligence techniques for defensive deception: a review, recent advances, open problems and future directions / P. V. Mohan, S. Dixit, A. Gyaneshwar [et al.] // Sensors. – 2022. – V. 22, No. 6.

66. De Gaspari F. Towards intelligent cyber deception systems / F. De Gaspari, S. Jajodia, L. V. Mancini [et al.] // Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings. – 2019. – P. 21-33.

67. Heckman K. E. Intrusions, Deception, and Campaigns / K. E. Heckman, F. J. Stech, R. K. Thomas // Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense. – 2015. – P. 31-52.

68. Achleitner S. Cyber deception: Virtual networks to defend insider reconnaissance / S. Achleitner, T. La Porta, P. McDaniel // Proceedings of the 8th ACM CCS international workshop on managing insider security threats. – 2016. – P. 57-68.

69. Zhang L., Thing V. L. L. Three decades of deception techniques in active cyber defense-retrospect and outlook / L. Zhang, V. L. L. Thing // Computers & Security. – 2021. – V. 106.

70. Lu Z. Cyber deception for computer and network security: Survey and challenges / Z. Lu, C. Wang, S. Zhao // arXiv. – 2020.

71. Jay D. Deception technology based intrusion protection and detection mechanism for digital substations: a game theoretical approach // IEEE Access. – 2023. – V. 11. – P. 53301-53314.

72. Srinivasa S. Towards systematic honeytoken fingerprinting / S. Srinivasa, J. M. Pedersen, E. Vasilomanolakis // 13th International Conference on Security of Information and Networks. – 2020. – P. 1-5.

73. Han X., Kheir N., Balzarotti D. Deception techniques in computer security: A research perspective // ACM Computing Surveys (CSUR). – 2018. – V. 51. – №. 4. – P. 1-36.

74. Maddireddy B. R. Enhancing Network Security through AI-Powered Automated Incident Response Systems / B. R. Maddireddy, B. R. Maddireddy // International Journal of Advanced Engineering Technologies and Innovations. – 2023. – V. 1, No. 2. – P. 282-304.

75. Aggarwal P. Cyber-security: role of deception in cyber-attack detection / P. Aggarwal, C. Gonzalez, V. Dutt // Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity – 2016. – P. 85-96.

76. Dark Reading. Cyber Deception Reduces Data Breach Costs by Over 51% & SOC Inefficiencies by 32% [Электронный ресурс]. – URL: https://www.darkreading.com/vulnerabilities-threats/cyber-deception-reduces-data-breach-costs-by-over-51-soc-inefficiencies-by-32- (дата обращения: 19.09.2024).

77. Lei C. Moving target defense techniques: A survey / C. Lei, H. Q. Zhang, J. L. Tan // Security and Communication Networks. – 2018. – V. 2018, No. 1.

78. Zhuang R. Towards a theory of moving target defense / R. Zhuang, S. A. DeLoach, X. Ou // Proceedings of the first ACM workshop on moving target defense. – 2014. – P. 31-40.

79. Khosravi-Farmad M. Moving target defense against advanced persistent threats for cybersecurity enhancement / M. Khosravi-Farmad, A. A. Ramaki, A. G. Bafghi // 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE). – 2018. – P. 280-285.

80. Okhravi H. Moving target techniques: Leveraging uncertainty for cyber defense / H. Okhravi, W. W. Streilein, K. S. Bauer // Lincoln Laboratory Journal. – 2016. – V. 22, No. 1. – P. 100-109.

81. Cho J. H. Toward proactive, adaptive defense: A survey on moving target defense / J. H. Cho, D. P. Sharma, H. Alavizadeh [et al.] //I EEE Communications Surveys & Tutorials. – 2020. – V. 22, No. 1. – P. 709-745.

82. Escaleira P. Moving Target Defense for the cloud/edge Telco environments / P. Escaleira, V. A. Cunha, D. Gomes [et al.] // Internet of Things. – 2023. – V. 24.

83. Wang L. Moving target defense against network reconnaissance with software defined networking / L. Wang, D. Wu // Information Security: 19th International Conference (ISC 2016). – 2016. – P. 203-217.

84. Bardas A. G. MTD CBITS: Moving target defense for cloud-based IT systems / A. G. Bardas, S. C. Sundaramurthy, X. Ou [et al.] // Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security. – 2017. – P. 167-186.

85. Sengupta S. Moving target defense: a symbiotic framework for AI & security // Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems. – 2017. – P. 1861-1862.

86. Husain M. I. Lightweight reconfigurable encryption architecture for moving target defense / M. I. Husain, K. Courtright, R. Sridhar // 2013 IEEE Military Communications Conference (MILCOM 2013). – 2013. – P. 214-219.

87. Zhang Z. FPGA-oriented moving target defense against security threats from malicious FPGA tools / Z. Zhang, Q. Yu, L. Njilla [et al.] // 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). – 2018. – P. 163-166.

88. Casola V. A moving target defense approach for protecting resource-constrained distributed devices / V. Casola, A. De Benedictis, M. Albanese // 2013 IEEE 14th International Conference on Information Reuse & Integration (IRI). – 2013. – P. 22-29.

89. DeLoach S. A. Model-driven, moving-target defense for enterprise network security / S. A. DeLoach, X. Ou, R. Zhuang [et al.] // Models@ run. time: Foundations, Applications, and Roadmaps. – 2014. – P. 137-161.

90. Xu X. An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector / X. Xu, H. Hu, Y. Liu // Security and Communication Networks. – 2021. – V. 2021, No. 1.

91. Jalowski Ł. A survey on moving target defense for networks: A practical view / Ł. Jalowski, M. Zmuda, M. Rawski // Electronics. – 2022. – V. 11, No. 18.

92. 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.

93. Kampanakis P. SDN-based solutions for moving target defense network protection / P. Kampanakis, H. Perros, T. Beyene // Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. – 2014. – P. 1-6.

94. Наливайко А. Защита с использованием подвижных целей (Moving Target Defense): описание технологии и краткий обзор решений [Электронный ресурс]. – URL: https://www.anti-

malware.ru/analytics/Market_Analysis/protection-with-Moving-Target-Defense (дата обращения: 19.09.2024).

95. Diogenes Y. Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics / Y. Diogenes, E. Ozkaya. – Packt Publishing Ltd, 2018. – 353 p.

96. Cai G. L. Moving target defense: state of the art and characteristics / G. L. Cai, B. S. Wang, W. Hu [et al.] // Frontiers of Information Technology & Electronic Engineering. – 2016. – V. 17, No. 11. – P. 1122-1153.

97. Roy I. Study on network scanning using machine learning-based methods / I. Roy, S. Sonthalia, T. Mandal [et al.] // Proceedings of International Ethical Hacking Conference 2019 (eHaCON 2019). – 2020. – P. 77-85.

98. ФСТЭК России. Банк данных угроз безопасности информации [Электронный ресурс]. – URL: https://bdu.fstec.ru/ (дата обращения: 19.09.2024).

99. Roy S. Survey and taxonomy of adversarial reconnaissance techniques / S. Roy, N. Sharmin, J. C. Acosta [et al.] // ACM Computing Surveys. – 2022. – V. 55, No. 6. – P. 1-38.

100. Pinkard B. Nmap in the Enterprise: Your Guide to Network Scanning / B. Pinkard, A. Orebaugh // syngress, United State Of America. – 2008. – 245 p.

101. Positive Technologies. Прочитай и сделай: проводим сканирование сети самостоятельно [Электронный ресурс]. – URL: https://habr.com/ru/companies/pt/articles/513776/ (дата обращения: 19.09.2024).

102. Shaw R. Literature Review on Packet Sniffing: Essential for Cybersecurity & Network Security / R. Shaw, S. Parveen // 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). – 2024. – P. 715-719.

103. Velan P. A survey of methods for encrypted traffic classification and analysis / P. Velan, M. Čermák, P. Čeleda [et al.] // International Journal of Network Management. – 2015. – V. 25, No. 5. – P. 355-374.

104. Asrodia P. Analysis of various packet sniffing tools for network monitoring and analysis / P. Asrodia, H. Patel // International Journal of Electrical, Electronics and Computer Engineering. – 2012. – V. 1, No. 1. – P. 55-58.

105. So-In C. A survey of network traffic monitoring and analysis tools // Cse 576m computer system analysis project, Washington University in St. Louis. – 2009.

106. De Montigny-Leboeuf A. Passive network discovery for real time situation awareness / A. De Montigny-Leboeuf, F. Massicotte // Proceedings of the The RTO Information Systems Technology Panel (IST) Symposium on Adaptive Defence in Unclassified Networks. – 2004. – P. 288-300.

107. Anu P. A survey on sniffing attacks on computer networks / P. Anu, S. Vimala // 2017 International Conference on Intelligent Computing and Control (I2C2). – 2017. – P. 1-5.

108. RFC 7348. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks [Электронный ресурс]. – URL: https://www.rfc-editor.org/rfc/rfc7348.html (дата обращения: 19.09.2024).

109. Jain V. Troubleshooting Cisco Nexus Switches and NX-OS / V. Jain, B. Edgeworth, R. Furr. – Cisco Press, 2018. – 1072 p.

110. JSON-RPC Working Group. JSON-RPC 2.0 Specification [Электронный ресурс]. – URL: https://www.jsonrpc.org/specification (дата обращения: 19.09.2024).

111. Lasocha W. P. Comparison of WebSocket and HTTP protocol performance / W. P. Lasocha, M. Badurowicz // Journal of Computer Sciences Institute. – 2021. – V. 19.

112. Petersen R. Ubuntu 22.04 LTS Desktop: Applications and Administration. – surfing turtle press, 2022. – 656 p.

113. Кушко Е.А. Исходный код программного обеспечения метода защиты локальной сети передачи данных от исследования на основе реконфи-

гурации топологии сетевого уровня [Электронный ресурс]. – URL: https://github.com/ekushko/qt-vxlan-mtd (дата обращения: 19.09.2024).

114. Tundis A. A review of network vulnerabilities scanning tools: Types, capabilities and functioning / Tundis A., Mazurczyk W., Mühlhäuser M. // Proceedings of the 13th international conference on availability, reliability and security. – 2018. – P. 1-10.

115. Hara K. Analysis of function of rectified linear unit used in deep learning / K. Hara, D. Saito, H. Shouno // 2015 international joint conference on neural networks (IJCNN). – 2015. – P. 1-8.

116. 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.

117. 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.

118. Xu X. Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack / X. Xu, H. Hu, Y. Liu [et al.] // Digital Communications and Networks. – 2022. – V. 8, No. 3. – P. 373-387.

119. Кушко Е.А. Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. – 2020. – № 4(52). – С. 39–52.

120. Putra C. A. Point to Point Protocol Tunneling VPN Simulation and Analysis on Sniffing / C. A. Putra, Y. V. Via, W. S. J. Saputra // International Conference on Science and Technology (ICST 2018). – 2018. – P. 1094-1097.

121. Guernsey D. Security analysis of the MPLS label distribution protocol / D. Guernsey, A. Engel, J. Butts [et al.] // Critical Infrastructure Protection IV: Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Revised Selected Papers 4. – 2010. – P. 127-139.

122. НПП «Цифровые решения». Современные решения для построения систем информационной безопасности — брокеры сетевых пакетов (Network Packet Broker) [Электронный ресурс]. – URL: https://habr.com/ru/companies/dsol/articles/490252/ (дата обращения: 19.09.2024).

123. Пескова О. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет / О. Ю. Пескова, Г. Ю. Халабурда // Материалы Всероссийской объединенной конференции «Интернет и современное общество». Санкт- Петербург, 10–12 октября, 2012. С. 348–354.

124. International Telecommunication Union Telecommunication Standardization Sector (ITU-T). Ethernet service activation test methodology [Электронный ресурс]. – URL: https://www.itu.int/rec/T-REC-Y.1564-201602-I/en (дата обращения: 16.12.2024).

125. Zhang M. Network attack surface: Lifting the concept of attack surface to the network level for evaluating networks' resilience against zero-day attacks / M. Zhang, L. Wang, S. Jajodia [et al.] // IEEE Transactions on Dependable and Secure Computing. – 2018. – V. 18, No. 1. – P. 310-324.

126. Aydeger A. A moving target defense and network forensics framework for ISP networks using SDN and NFV / A. Aydeger, N. Saputro, K. Akkaya // Future Generation Computer Systems. – 2019. – V. 94. – P. 496-509.

127. Zhao Z. An SDN-based fingerprint hopping method to prevent fingerprinting attacks / Z. Zhao, F. Liu, D. Gong // Security and Communication Networks. – 2017. – V. 2017, No. 1.

128. Rawski M. Network topology mutation as moving target defense for corporate networks // International Journal of Electronics and Telecommunications. – 2019. – V. 65.

129. Venkatesan S. et al. A moving target defense approach to mitigate DDoS attacks against proxy-based architectures / S. Venkatesan, M. Albanese, K.

Amin [et al.] // 2016 IEEE conference on communications and network security (CNS). – 2016. – P. 198-206.

130. 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.

131. Skowyra R. Have no PHEAR: Networks without identifiers / R. Skowyra, K. Bauer, V. Dedhia [et al.] // Proceedings of the 2016 ACM workshop on moving target defense. – 2016. – P. 3-14.

132. Jafarian J. H., Al-Shaer E., Duan Q. An effective address mutation approach for disrupting reconnaissance attacks / J. H. Jafarian, E. Al-Shaer, Q. Duan // IEEE Transactions on Information Forensics and Security. – 2015. – V. 10, No. 12. – P. 2562-2577.

133. Саломатин С. Б. Моделирование алгоритмов быстрой обработки сигналов в инфокоммуникационных сетях: учебно-методическое пособие. – 2016.

134. Nmap Security Scanner. Опции управления временем и производительностью [Электронный ресурс]. – URL: https://nmap.org/man/ru/man-performance.html (дата обращения: 27.12.2024).

135. Ворончихин И. С. Маскирование структуры распределенных информационных систем в киберпространстве / И. С. Ворончихин, И. И. Иванов, Р. В. Максимов, С. П. Соколовский // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 92-101.

136. Красов А. В. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях / А. В. Красов, Р. Б. Петрив, Д. В. Сахаров [и др.] // Труды учебных заведений связи. – 2019. – Т. 5, № 3. – С. 86-97.

ПРИЛОЖЕНИЕ 1. Протокол взаимодействия с сетевым оборудованием

Название	Тип	Формат

Ввод команды на исполнение	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "cli_ascii",
		"params": {
		"cmd": "<команда>",
		"version": 1
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": null
		}

	Сообщение об ошибке	400 Bad Request

ПРИЛОЖЕНИЕ 2. Протокол взаимодействия с хостами

Название	Тип	Формат

Установка параметров виртуального сетевого адаптера	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "setupInterface<индекс>",
		"params": {
		"interface": "<имя интерфейса>",
		"ip": "<IP-адрес>",
		"mac": "<MAC-адрес>",
		"mask": <маска>,
		"routes": [
		{
		"metric": <метрика>,
		"gateway": "<IP-адрес шлюза>",
		"mask": <маска>,
		"network": "<целевая подсеть>"
		}
		],
		"vlanId": <метка группы>
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": <результат выполнения: true – выполнено, false – не выполнено>
		}

	Сообщение об ошибке	{
		"error": {
		"code": <код ошибки>,
		"message": "<сообщение об ошибке>"
		},
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0"
		}

Очистка параметров виртуального сетевого адаптера	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "clearInterface<индекс>",
		"params": {
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": <результат выполнения: true – выполнено, false – не выполнено>
		}

	Сообщение об ошибке	{
		"error": {
		"code": <код ошибки>,
		"message": "<сообщение об ошибке>"
		},
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0"
		}

Установка списка доменных имен и соответствующих им адресов	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "setupHosts",
		"params": {
		"hosts": [
		{
		"domainName": "<доменное имя>",
		"ip": "<IP-адрес>"
		}
		]
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": <результат выполнения: true – выполнено, false – не выполнено>
		}

	Сообщение об ошибке	{
		"error": {
		"code": <код ошибки>,
		"message": "<сообщение об ошибке>"
		},
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0"
		}

Ввод установленных параметров виртуальных сетевых адаптеров и списка доменных имен и соответствующих им адресов	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "applyNetplan",
		"params": {
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": <результат выполнения: true – выполнено, false – не выполнено>
		}

	Сообщение об ошибке	{
		"error": {
		"code": <код ошибки>,

		"message": "<сообщение об ошибке>" }, "id": <идентификатор запроса>, "jsonrpc": "2.0" }

Проверка наличия соединения	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "checkConnection",
		"params": {
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": <результат выполнения: true – выполнено, false – не выполнено>
		}

	Сообщение об ошибке	{
		"error": {
		"code": <код ошибки>,
		"message": "<сообщение об ошибке>"
		},
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0"
		}

Получить список потенциально опасных хостов	Запрос	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"method": "getScanners",
		"params": {
		}
		}

	Ответ	{
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0",
		"result": {
		"scanners": [
		{ "ip": "<IP-адрес>" }
		]
		}
		}

	Сообщение об ошибке	{
		"error": {
		"code": <код ошибки>,
		"message": "<сообщение об ошибке>"
		},
		"id": <идентификатор запроса>,
		"jsonrpc": "2.0"
		}

ПРИЛОЖЕНИЕ 3. Свидетельства о регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022680466

Программный модуль реализации защищенного обмена данными на основе динамической топологии сети

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» (СибГУ им. М.Ф. Решетнева) (RU)***

Автор(ы): ***Кушко Евгений Александрович (RU)***

Заявка № **2022669450**
Дата поступления **18 октября 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***01 ноября 2022 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

ПРИЛОЖЕНИЕ 4. Акты внедрения

Акционерное общество
«Научно-производственное предприятие «Радиосвязь»
(АО «НПП «Радиосвязь»)
ул. Декабристов, д.19, Красноярск, 660021
Тел. (391) 204-11-02, тел./факс (391) 204-12-38 E-mail: info@krtz.su
ОКПО 44589548, ОГРН 1122468072231, ИНН/КПП 2460243408/246001001

УТВЕРЖДАЮ
Заместитель Генерального директора
по научно-техническому развитию
АО «НПП «Радиосвязь»
_____ Е.В. Богатырев
«___»_____20___ г.

АКТ

о внедрении результатов диссертационной работы
Кушко Евгения Александровича,
представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Комиссия в составе: председателя – главного конструктора А.А. Казакова; и членов комиссии: начальника отдела ПД ИТР и ТЗИ М.В. Тарасевича; начальника отдела систем управления А.В. Мишанова; ведущего инженера-конструктора отдела систем управления А.А. Адамовича, составили настоящий акт о том, что результаты диссертационной работы Е.А. Кушко на тему «Метод защиты от стороннего исследования локальной сети передачи данных на основе реконфигурации топологии сетевого уровня» были внедрены в стенд, имитирующий станцию наземной связи. Программное средство, которое реализует предложенные метод и алгоритм, было

применено для защиты сети управления каналообразующим и модемным оборудованием станции.

По результатам внедрения получено следующее:

1. В ходе испытаний установлено, что метод защиты сети от стороннего исследования и алгоритм формирования топологии сетевого уровня потенциально применимы для защиты наземной станции связи от исследования злоумышленником: на каждой итерации метода информация о сети (физический адрес, логический адрес, логическая топология сети и маршруты передачи) не соответствует ранее собранной информации на предыдущих итерациях.

2. В ходе испытаний зафиксированы значительные задержки (от 30 до 46 секунд) при смене одной топологии сетевого уровня на другую, что делает текущую реализацию метода применимой только для ограниченного набора схем организации связи, не требующих малых задержек. Задержки возникают из-за того, что изменения конфигураций на стороне сетевого оборудования требуют времени, которое соответствует полученным задержкам. Для полноценного применения предложенного метода для защиты от стороннего исследования необходимо, чтобы сетевое оборудование было способно применять новые конфигурации быстрее, чем в текущем его состоянии.

Тем не менее предложенный метод является перспективным, так как испытания показали, что метод позволяет защитить сеть от стороннего исследования, и в дальнейшем, с развитием сетевого оборудования, предложенный метод может получить более широкое применение.

Председатель комиссии: А.А. Казаков

Члены комиссии: М.В. Тарасевич

А.В. Мишанов

А.А. Адамович

МИНИСТЕРСТВО НАУКИ И
ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное
образовательное учреждение
высшего образования
**«Сибирский государственный
университет науки и технологий
имени академика М.Ф. Решетнева»
(СибГУ им. М.Ф. Решетнева)
Институт информатики и
телекоммуникаций
(ИИТК)**
просп. им. газеты «Красноярский рабочий», 31
г. Красноярск, 660014
Тел.: (391) 264-00-14. Факс: (391) 264-47-09
E-mail: info@sibsau.ru
http://www.sibsau.ru
ОКПО 02069734, ОГРН 1022402056038
ИНН/КПП 2462003320/246201001
_____№ _____

Акт внедрения

Результаты, полученные в ходе проведения Кушко Е. А. диссертационного исследования «Метод защиты от стороннего исследования локальной сети передачи данных на основе реконфигурации топологии сетевого уровня» в рамках гранта Минцифры России № 40469-07/2021-К «Грант ИБ» (автор является единоличным исполнителем) были внедрены в учебный процесс в следующем объеме:

Внедрение результатов диссертационной работы в учебный процесс института информатики и телекоммуникаций для направлений подготовки 10.03.01 «Информационная безопасность», 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.02 «Информационная безопасность телекоммуникационных систем» в рамках предметов «Сети и системы передачи информации» и «Безопасность облачных технологий».

Комплект практических заданий и дополнительных материалов для указанных выше предметов, демонстрирующий методы защиты от стороннего исследования при различных стратегиях атакующего. Предложенный в диссертационной работе метод демонстрирует защищенность от стороннего исследования.

Директор ИИТК К.В. Сафонов

ПРИЛОЖЕНИЕ 5. Дипломы и награды

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

Диплом

III степени

НАГРАЖДАЕТСЯ

Кушко

Евгений Александрович

За доклад, представленный в финале XVII Всероссийского конкурса-конференции студентов и аспирантов по информационной безопасности «SIBINFO-2017»

Председатель оргкомитета,
ректор ТУСУР, директор Института
системной интеграции и безопасности,
д-р техн. наук, профессор А.А. Шелупанов

Томск 20 апреля 2017 г.

МТУСИ

ДИПЛОМ ПОБЕДИТЕЛЯ

Всероссийского конкурса научных проектов аспирантов, соискателей и молодых ученых на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики

выдан

КУШКО
ЕВГЕНИЮ АЛЕКСАНДРОВИЧУ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

Врио ректора МТУСИ Е.В. Титов

Москва 2021