УДК 004.056.53

Метод реализации защищенного обмена данными на основе динамической топологии сети

Е. А. Кушко

Данная работа посвящена противодействию перехвату и анализу сетевого трафика. В работе рассмотрена статистика инцидентов информационной безопасности, связанная с хакерскими атаками на информационные системы предприятий, проанализированы требования регуляторов, связанные с обеспечением защищенного обмена данными по сети и сетевой безопасности в целом, а также приведено сравнение существующих решений по обеспечению защищенной передачи данных и противодействию несанкционированному перехвату и анализу сетевого трафика, и решения, обеспечивающие сокрытие структуры и конфигурации информационной системы. Также в работе представлен собственный метод реализации защищенного обмена данными на основе динамической топологии сети, который отличается от известных решений способом сокрытия сторон сетевого взаимодействия. Данный метод применен в сенсорной сети для сокрытия её архитектуры и конфигурации от злоумышленника.

Ключевые слова: локальная сеть, защищенный обмен данными, протокол передачи данных, технология защиты движущейся цели.

1. Введение

Средства защиты, как правило, работают на границах между сетями или сегментами одной сети, поэтому в случае их преодоления злоумышленник трудно детектируем. В результате злоумышленник практически не ограничен во времени и имеет возможность тщательно спланировать свою атаку.

Предлагается новый метод реализации защищенного обмена данными на основе динамической топологии сети, в результате применения которого защищены не только передаваемые данные, но и участники сетевого взаимодействия: передаваемые пакеты данных явно не содержат данные об источнике и получателе, а также предусмотрено реконфигурирование системы, в результате чего злоумышленник не может обладать долгосрочной информацией о структуре и конфигурации информационной системы, при этом не изменяется работа других сетевых сервисов, которые не демаскируют защищаемую функцию узла.

Объектом исследования является передача данных внутри локальной сети. Предметом исследования является защищенный обмен данными внутри локальной сети. Целью исследования является повышение уровня защищенности сторон межсетевого обмена. Для этого необходимо проанализировать статистику инцидентов информационной безопасности и требования регуляторов по информационной безопасности, сравнить существующие решения в этой области, выявить их преимущества и недостатки, и на основе этих данных разработать и реализовать собственное решение, а также апробировать это решение на прикладной задаче обеспечения безопасности сенсорной сети, протестировать это решение и оценить его эффективность.

2. Анализ статистики инцидентов информационной безопасности

В аналитике компании Positive Technologies за 2019 год приводятся следующие данные: 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, и, как правило, на первом этапе после проникновения злоумышленник осуществляет сетевую разведку [1].

Компания Positive Technologies в аналитике за 2018 год говорит о том, что значительную долю уязвимостей внутренних локальных вычислительных сетей предприятий составляют недостатки защиты протоколов сетевого и канального уровней, что приводит к перенаправлению трафика и перехвату информации о конфигурации сети, а также уязвимости, связанные с использованием незащищенных протоколов передачи данных [2].

Статистика компании Infowatch 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 % [3].

По статистике компании JSOC, все больший интерес для злоумышленников начинают представлять схемы сетей, особенности работы информационных систем, которые в дальнейшем используются при планировании и подготовке последующих атак и мошеннических схем [4]. По статистике центра мониторинга «Перспективный мониторинг», около 19 % зарегистрированных событий связаны со сканированием сети [5].

Опыт компании Positive Technologies говорит о том, что большинство средств обнаружения и предотвращения вторжений закрывает лишь 10% уязвимостей, содержащихся в базе CVE (Common Vulnerabilities and Exposures). Как отмечают специалисты компании, одна из причин – это нежелание вендоров и экспертов делиться техническими деталями обнаруженных уязвимостей. Например, для разработки правил для средств обнаружения и предотвращения вторжений необходимы дампы сетевого трафика, которые содержат эксплуатацию уязвимости, – эти данные ускорили бы разработку необходимых правил. Это актуально не только для средств обнаружения и предотвращения вторжений, но и для других средств защиты информации [6].

Несмотря на то, что всё больше организаций начинают заниматься вопросами защиты информации и наблюдается тенденция увеличения бюджетов, затрачиваемых на построение систем защиты, применяемых мер оказывается недостаточно. Злоумышленники в большинстве случаев успешно проникают во внутреннюю сетевую инфраструктуру, а противодействовать злоумышленнику, который находится внутри локальной вычислительной сети, большинство предприятий не может. Как правило, на первоначальном этапе после проникновения злоумышленник занимается изучением локальной вычислительной сети для сбора данных, необходимых ему для осуществления эффективной атаки. Сетевая разведка – это один из ключевых этапов атаки злоумышленника.

3. Анализ нормативной базы и требований регуляторов по защите информации

В данной работе необходимо рассмотреть требования и меры, касающиеся безопасности внутри инфраструктуры информационной системы, когда злоумышленник преодолел сетевой периметр и непосредственно находится в локальной вычислительной сети. Федеральной службой по техническому и экспортному контролю Российской Федерации (ФСТЭК) установлены следующие меры по обеспечению технической защиты внутри локальной сети, которые закреплены в приказе «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими

процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14 марта 2014 года № 31 [7]:

1) построение эшелонированной системы защиты;
2) сегментирование информационной системы;
3) управление сетевыми потоками;
4) сокрытие архитектуры и конфигурации информационной системы;
5) защита информации при её передаче по каналам связи;
6) обеспечение доверенных каналов и маршрутов;
7) обеспечение подлинности сетевых соединений;
8) управление сетевыми соединениями.

Построение эшелонированной системы защиты предполагает использование средств защиты на всех уровнях информационной системы: на конечных устройствах, на сетевом оборудовании, на каналах связи, на конечных устройствах и т.д. Сегментирование информационной системы подразумевает разделение сети на сегменты, на границах которых располагаются средства защиты информации для того, чтобы злоумышленнику пришлось преодолеть не только внешний периметр информационной системы, но и периметр каждого сегмента сети. Управление сетевыми потоками необходимо для организации доступа к сетевым ресурсам таким образом, чтобы обеспечивались конфиденциальность, целостность и доступность.

Сокрытие архитектуры и конфигурации информационной системы, как правило, достигается организационными мерами в совокупности с технической защитой периметра сети или её сегмента, поскольку на текущий момент не существует сертифицированных средств, а несертифицированные средства неприменимы. Защита информации при её передаче по каналам связи предполагает шифрование, а также доверенный канал должен обеспечиваться при доступе к информационной системе. Обеспечение подлинности сетевых соединений достигается путем применения аутентификации и контроля целостности передаваемых данных. Управление сетевыми соединениями предполагает фильтрацию сетевых пакетов и контроль обращений к узлам.

Приказ ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 года № 21 [8] устанавливает меры, такие как: сегментирование информационной системы; обеспечение защиты персональных данных при её передаче от раскрытия, модификации и навязывания; обеспечение доверенных канала и маршрута между администратором, пользователем и средствами защиты информации; контроль санкционированного и исключение несанкционированного доступа к ресурсам и информации; защита беспроводных соединений путем контроля подключения к беспроводным сетям, ограничение их использования исходя из необходимости и т.д. Основные меры, изложенные в данном приказе, заключаются в обеспечении защиты периметра сети и её сегментов, обеспечении контроля и управления информационными потоками и сетевыми подключениями, а также использовании шифрования при передаче данных.

Приказ ФСТЭК «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года № 17 [9] также устанавливает меры, касающиеся: сегментирования сети и защиты их периметров техническими средствами; обеспечения доверенных каналов и маршрутов; контроля санкционированного и исключения несанкционированного доступа к ресурсам и информации; подтверждения источников информации, передаваемой по сети; обеспечения подлинности сетевых соединений; защиты беспроводных сетей. Но данный приказ также содержит меру: воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характери-

стиках информационной системы, которая является необязательной, поскольку, как указано выше, на текущий момент нет сертифицированных средств по выполнению мер такого рода.

Методический документ ФСТЭК по мерам защиты информации в ГИС [10], стандарт ИСО/МЭК 27002 [11], серия стандартов ИСО/МЭК 27033 [12] и стандарт Банка России СТО БР ИББС-1.0-2014 [13] определяют и устанавливают требования и рекомендации по реализации мер и средств контроля и управления сетевой безопасностью, а также предоставляют подробные рекомендации по аспектам безопасности управления, функционирования и использования сетей информационных систем и их соединений. Эти стандарты также предлагают комплексный подход к защите внутренних локальных вычислительных сетей: ограничение доступа к ресурсам и к локальной вычислительной сети в целом, сегментирование сети и обеспечение защиты периметров, использование шифрования при передаче данных, а также исключение несанкционированного доступа и контроль санкционированного доступа на всех уровнях информационной системы.

Международный опыт, изложенный в стандартах, таких как PCI DSS [14] и SP 800-47 «Security Guide for Interconnecting Information Technology Systems» [15], также предполагает комплексный подход к обеспечению технической защиты локальных вычислительных сетей информационных систем.

В целом требования и рекомендации регуляторов по защите информации, изложенные в вышеупомянутых стандартах и методических документах по обеспечению безопасности локальных вычислительных сетей информационных систем, предполагают комплекс технических мер, а именно:

1) использование средств защиты на периметре информационной системы;

2) сегментирование локальной вычислительной сети и использование средств защиты на периметрах её сегментов;

3) использование средств защиты на всех уровнях информационной системы (конечное оборудование, сетевое оборудование и так далее);

4) контроль и управление сетевыми потоками и соединениями;

5) обеспечение доверенных каналов и маршрутов;

6) обеспечение подлинности сетевых соединений и подтверждения источников данных;

7) контроль санкционированного и исключение несанкционированного доступа к узлам и ресурсам;

8) применение шифрования данных и использование защищенных каналов связи.

Также регуляторы в качестве необязательной меры рекомендуют осуществлять сокрытие архитектуры и конфигурации информационной системы, однако сертифицированных технических средств на текущий момент нет, поэтому разработка подобных средств сейчас востребована.

4. Анализ существующих решений по обеспечению защищенной передачи данных

Классическим подходом по обеспечению защищенного обмена данными внутри локальной сети является сегментирование сети и использование средств защиты информации, таких как межсетевые экраны, средства обнаружения и предотвращения вторжений и других, на периметре локальной вычислительной сети и на периметрах её сегментов. Также к классическим мерам можно отнести построение коммутируемой инфраструктуры и шифрование. Под коммутируемой инфраструктурой следует понимать такую физическую архитектуру сети, при которой каждое устройство, подключенное к сетевому оборудованию, имеет доступ только к необходимым узлам, данным и трафику.

Классические решения по обеспечению защищенного обмена данными внутри локальной сети достаточно широко применяются, так как являются базовыми и обязательными для большинства категорий информационных систем. Однако классический набор мер имеет не-

достатки. Во-первых, данные меры имеют апробированные способы и средства их обхода и доступны для изучения [16–17]. Во-вторых, применение этих средств требует квалифицированного персонала, который постоянно должен реагировать на инциденты, осуществлять обновления программного обеспечения и правил безопасности, быть постоянно готовым к потенциальной атаке, то есть постоянно сопровождать информационную систему и защищать её. Как показывает статистика, злоумышленники могут преодолеть периметр безопасности, и их выявление становится крайне затруднительным. Шифрование позволяет защитить данные при передаче, однако оно не скрывает факт передачи данных между узлами. Кроме того, злоумышленник может установить даже тип передаваемых данных [18]. Конфигурация и архитектура большинства сетей доступна для изучения злоумышленником, и, как правило, они статичны – в результате злоумышленник неограничен во времени.

Для того, чтобы решить проблемы классических мер по обеспечению защищенного обмена данными внутри локальной сети, исследователи разработали ряд средств, таких как:

1) сетевая стеганография;

2) децентрализованные анонимные сети;

3) технология движущейся цели.

Сетевая стеганография направлена на сокрытие факта передачи данных. Как правило, данные скрываются в элементах управления протоколов связи и в простых пакетах данных. Методы сетевой стеганографии направлены на модификацию данных в заголовках и полях полезной нагрузки сетевых пакетов и на изменение структуры передачи пакетов. Некоторые методы сетевой стеганографии изменяют очередность передачи пакетов или осуществляют преднамеренную потерю пакетов при их передаче. Сетевая стеганография осуществляет передачу без изменения информации, при этом не нарушается функциональность сетевых сервисов. Однако этот метод сложен в реализации и использовании, а также имеет ограничения на объем передаваемой информации [19].

Децентрализованная анонимная сеть – это самоорганизующаяся адаптивная динамическая сеть. Примерами таких сетей являются i2p, tor и freenet. Такие сети предназначены для того, чтобы невозможно было установить отправителя и получателя данных сторонним наблюдателем. Децентрализованные анонимные сети широко используются для передачи данных через глобальную сеть. Данные защищены шифрованием, а маршруты передачи данных меняются через интервалы времени. Несмотря на это, многие сети позволяют скомпрометировать и модифицировать данные, идентифицировать участников обмена данными и перехватывать туннели передачи данных [20–21]. Однако их большими преимуществами являются самоадаптация, самоорганизация и самовосстановление. Такие системы трудно развернуть в локальной вычислительной сети, однако некоторые механизмы вполне применимы для организации защищенного обмена данными внутри неё: смена маршрутов передачи данных, смена ключей шифрования, выравнивание размеров пакетов и так далее.

Технология движущейся цели применяется для затруднения сетевой атаки злоумышленника путем периодичных изменений сети во времени, чтобы злоумышленник не мог обладать долгосрочной информацией о локальной вычислительной сети [22], при этом в результате этих изменений не должна нарушаться её работа. Злоумышленник при этом никак не ограничен в своих действиях. Схемы технологии движущейся цели обычно делятся на два типа: децентрализованная и централизованная. Как правило, децентрализованные схемы обладают более высоким уровнем защищенности [23]. Технология движущейся цели в основном используется в совокупности с криптографией. Однако эта технология находится на начальном этапе своего развития, область исследования слабо изучена, и только появляются первые технические решения [24–25].

Все существующие решения по обеспечению защищенного обмена данными имеют свои преимущества и недостатки, однако, как показывает статистика, для защиты локальной вычислительной сети их недостаточно. Злоумышленник успешно проникает внутрь сети и после трудно детектируем. В результате он неограниченно может изучать сеть, перехватывать и анализировать весь трафик, идентифицировать ключевые узлы. Существуют перспектив-

ные технологии, которые позволяют затруднить сетевую разведку злоумышленника, но они находятся на начальном этапе своего развития и имеют на данный момент существенные недостатки.

5. Формирование требований к разрабатываемому решению

Регуляторы в области информационной безопасности в методических и нормативных документах предлагают ряд мер, направленных на обеспечение безопасности локальных вычислительных сетей информационных систем. В общем случае меры заключаются в защите внешнего сетевого периметра информационной системы, разделении внутренней локальной вычислительной сети на сегменты и использовании средств защиты информации на их границах, исключении несанкционированного доступа к локальной вычислительной сети на всех её уровнях и построении защищенных каналов связи.

Однако по статистике инцидентов информационной безопасности злоумышленники успешно преодолевают сетевой периметр. Когда злоумышленник находится внутри локальной вычислительной сети, его детектирование трудновыполнимо. В результате злоумышленник может планировать свою атаку практически без ограничений во времени. Сетевая разведка – это один из основных этапов планирования атаки. Существуют технологии, направленные на создание условий дефицита информации о локальной вычислительной сети, в результате чего злоумышленник не может осуществить свою атаку.

В разрабатываемом решении необходимо учесть все существующие подходы и технологии по обеспечению безопасности локальных вычислительных сетей, их преимущества и недостатки. Разрабатываемое решение должно быть простым в развертывании и эксплуатации, автономным и самоадаптивным, не нарушать легитимную работу сети и другие требования безопасности. В результате был разработан стек протоколов защищенного обмена данными на основе динамической сети в качестве новой меры по обеспечению сокрытия конфигурации и архитектуры сенсорной сети, которая отличается от существующих методом сокрытия факта взаимодействия узлов в сети от стороннего наблюдателя.

6. Описание разрабатываемого решения

В основе разрабатываемого метода реализации защищенного обмена данными на основе динамической топологии сети лежат принципы технологии движущейся цели. Узлы, участвующие в защищенном обмене данными, перемещаются по мультикаст-группам и передают данные, используя групповое вещание. Каждый узел подключен одновременно к нескольким мультикаст-группам защищенного обмена данными и перенаправляет полученные данные во все группы, к которым он подключен, т.е. используется лавинная маршрутизация.

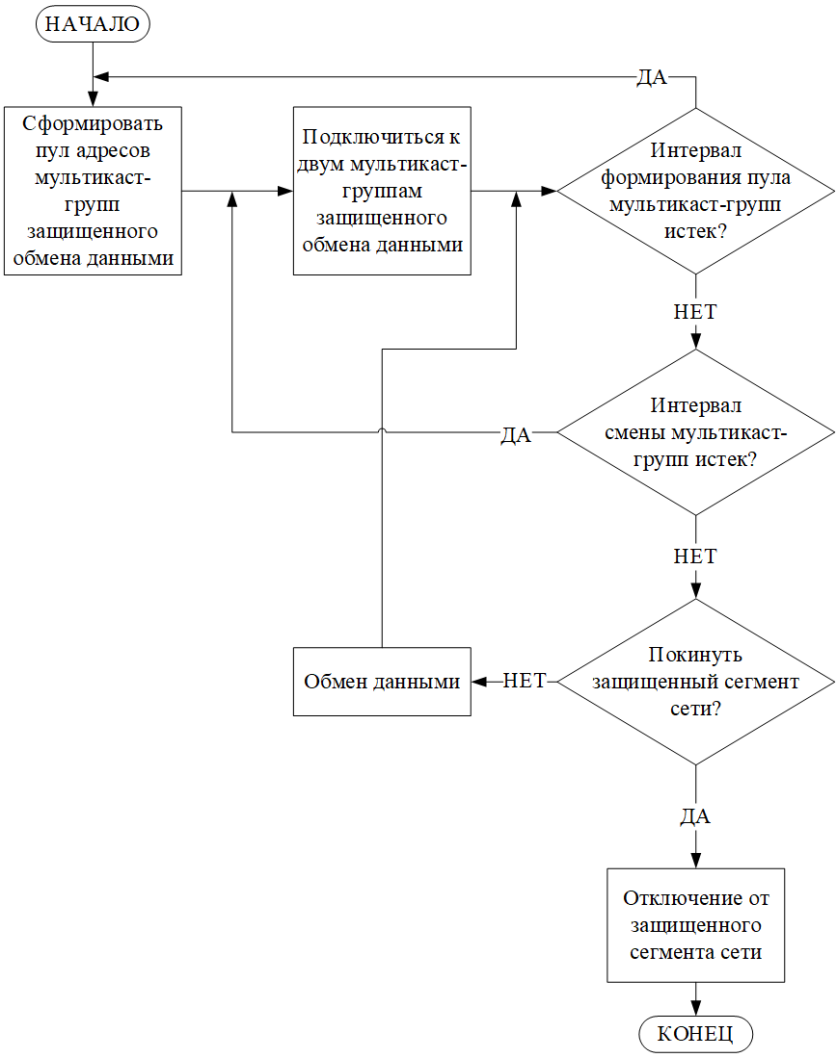

Рис. 1. Алгоритм инициализации защищенного обмена данными

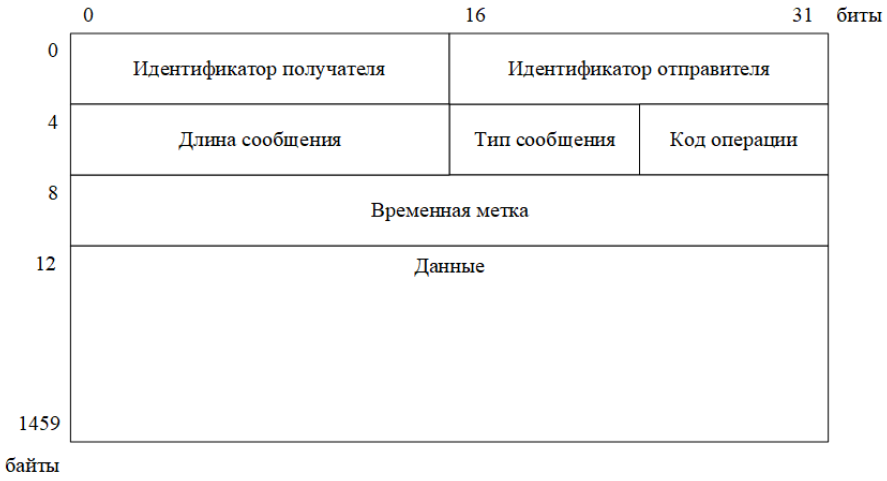

Рис. 2. Формат пакета данных

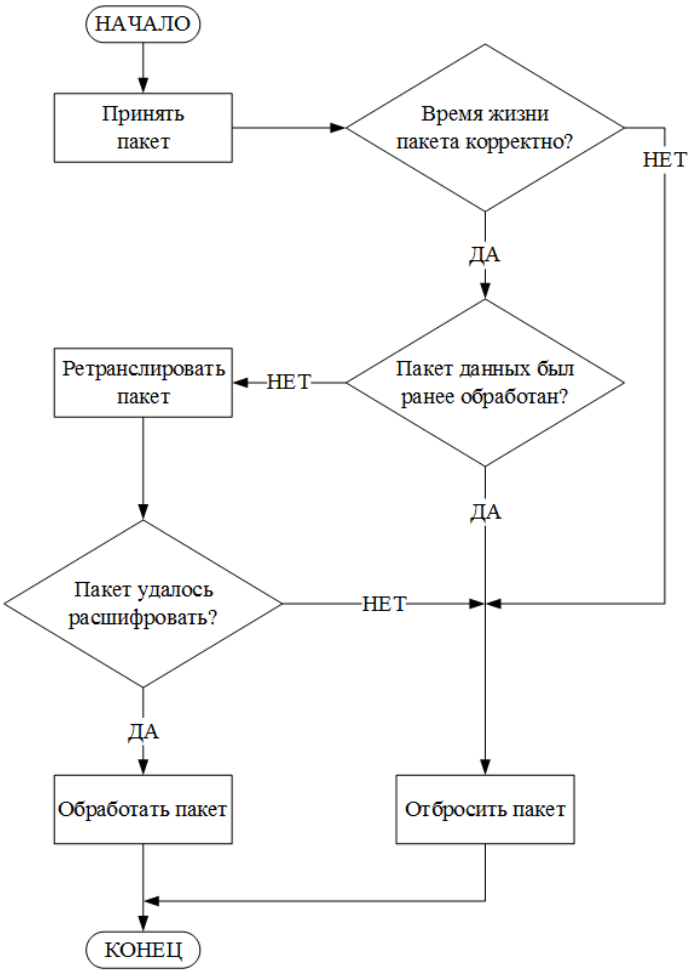

Рис. 3. Алгоритм обработки входящих пакетов данных

На этапе инициализации защищенного обмена, каждый узел-участник формирует пул адресов мультикаст-групп защищенного обмена данными, через которые осуществляется передача данных по алгоритму, зависящему от текущей даты и времени. Этот пул адресов меняется через определенные интервалы времени. Далее узел выбирает две мультикаст-группы и подключается к ним. По истечении другого временного интервала, который меньше, чем интервал переформирования пула адресов мультикаст-групп защищенного обмена данными, узел заново выбирает случайным образом мультикаст-группы. Общий алгоритм инициализации защищенного обмена данными представлен на рис. 1.

Для того чтобы передать данные, каждый узел-участник защищенного обмена данными формирует пакет данных, формат которого представлен на рис. 2, и передает его во все мультикаст-группы защищенного обмена данными, к которым он в данный момент подключен. Все пакеты данных имеют одинаковый размер, и в случае, если размер передаваемых данных превышает размер пакета, данные дробятся на несколько пакетов. Пакет шифруется открытым ключом получателя по алгоритму RSA с длиной ключа 1024 бит и содержит идентификаторы получателя и отправителя. Узлы, подключенные к мультикаст-группам защищенного обмена данными, в которые был отправлен пакет данных, ретранслируют этот пакет во все остальные мультикаст-группы и так далее.

После ретрансляции узел предпринимает попытку расшифровать заголовок пакета и извлечь из него свой идентификатор. В случае успешной расшифровки пакета данных узел обрабатывает пакет, в противном – отбрасывает его. Алгоритм обработки входящих пакетов данных представлен на рис. 3. Для того чтобы ретрансляция не была бесконечной, каждый пакет данных имеет время жизни. Кроме того, пакет отбрасывается в случае, если превышен максимальный размер пакета данных или пакет данных был ранее обработан узлом вне зависимости от того, предназначен он ему или нет.

При передаче данных таким образом злоумышленник, осуществляющий перехват и анализ передаваемых по сети данных, не может идентифицировать получателей и отправителей, так как пакеты данных не содержат в явном виде их IP-адреса. Пакет данных вне зависимости от объема передаваемых данных имеет фиксированный размер и зашифрован. Кроме того, участники защищенного обмена переключаются между мультикаст-группами защищенного обмена, логическая структура системы имеет динамическую топологию. Ретрансляция в совокупности с фиксированным размером пакета не позволит установить, какой пакет является запросом или ответом, а какой узел является источником или получателем. В результате злоумышленник не может установить потоки данных и взаимосвязи между узлами, а также не может обладать долгосрочной информацией о логической структуре системы.

7. Решение прикладной задачи обеспечения информационной безопасности

В качестве прикладной задачи выбрана задача обеспечения информационной безопасности сенсорной сети, а именно – техническое решение, реализующее меру «Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы» (ЗИС 8) из приказа ФСТЭК № 31 [7]. На практике данная мера реализуется организационными мерами и техническими средствами по предотвращению несанкционированного доступа в сеть по причине того, что на момент написания работы не существует сертифицированных технических средств по сокрытию архитектуры и конфигурации системы.

Сенсорная сеть – это беспроводная, самоконфигурируемая и распределенная сеть, которая решает задачи автоматизации, диагностики, телеметрии и межмашинного взаимодействия. Сенсорная сеть должна быть проста в развертывании и эксплуатации, не требовать частого техобслуживания, обладать высокой отказоустойчивостью и надежностью, а также функционировать на базе устройств с низкой производительностью в условиях невысокой пропускной способности.

В качестве протокола прикладного уровня выбран MQTT, который широко применятся в различных информационных системах – от умного дома до космической промышленности. Протокол MQTT отвечает всем требованиям, которые предъявляются к сенсорным сетям, и функционирует по принципу издатель-подписчик [26]. Итоговая система имеет следующую структуру:

1) протокол MQTT;
2) протокол инициализации обмена данными;
3) протокол конфигурирования системы;
4) протокол передачи и обмена данными.

MQTT содержит в себе три типа узлов: сервер-издатель, сервер-брокер и клиент-подписчик. Клиент-подписчик при подключении к защищенному сегменту сети генерирует пул мультикаст-групп защищенного обмена данными и выбирает две из них. В эти группы клиент-подписчик отправляет сообщение на создание защищенного соединения. Сервер-брокер, приняв запрос, по схеме Диффи–Хеллмана генерирует сеансовый ключ, и при помощи сеансового ключа клиент регистрируется на сервере-брокере, т.е. сообщает свой открытый ключ и идентификатор. В случае, если сеть содержит несколько серверов-брокеров, взаимодействие между клиентом-подписчиком и сервером-брокером осуществляется по принципу «кто первый ответит», а данные между серверами-брокерами о клиентах-подписчиках синхронизируются. Серверы-брокеры и серверы-издатели имеют встроенные ключи шифрования, так что дополнительная процедура аутентификации для них не осуществляется. Все данные MQTT инкапсулируются в пакет данных разрабатываемого решения и передаются по сети способом, описанным в предыдущей части данной работы.

Передача данных таким способом позволяет скрыть роль каждого узла в этой системе, так как объем трафика, передаваемый между узлами, распределен между всеми участниками системы и пакеты данных имеют одинаковый размер, а логическая структура системы изме-

няется через каждый интервал времени. Связи между конкретными узлами скрыты среди идентичных потоков данных, причем сами данные непосредственно защищены шифрованием, а отсутствие явной адресации повышает уровень общей защищенности.

8. Анализ эффективности передачи данных

Для проведения тестирования передачи данных собран тестовый стенд из 8 машин на базе беспроводного маршрутизатора Mikrotik RB941-2nD-TC для сигнала на частоте 2.4 ГГЦ и при скорости передачи данных до 300 Мбит/с: три сервера-издателя, два сервера-брокера и три клиента-подписчика, их характеристики приведены в табл. 1. Оценка эффективности строится на основе двух экспериментов: эксперимент на определение характера распределения пакетов внутри системы; определение характеристик производительности передачи данных. Также стоит отметить, что на данном этапе тестирование осуществляется для сценария QoS (quality of service, качество обслуживания) уровня 0, т.е. нет гарантированной доставки сообщения.

Таблица 1. Характеристики машин, участвующих в эксперименте

№	Роль	Технические характеристики	IP-адрес	Уровень сигнала (дБм)
1	сервер-издатель	Персональный компьютер на базе AMD Ryzen 5 3600 6c 12t 3.6-4.2 ГГц 16 Гб 3466 МГц DDR4 под управлением ОС Windows 10 x64	192.168.1.1	-61
2	сервер-издатель	Виртуальная машина Virtual Box Windows 7 x86 1 Гб ОЗУ на базе машины № 1	192.168.1.3	-61
3	сервер-издатель	Виртуальная машина Virtual Box на базе машины №1 Windows 7 x86 1 Гб ОЗУ	192.168.1.5	-61
4	сервер-брокер	Ноутбук на базе Intel Core i3 8130u 2c 4t 2.2-3.4 ГГц 8 Гб 2400 МГц DDR4 под управлением ОС Windows 10 x64	192.168.1.6	-57
5	сервер-брокер	Виртуальная машина Virtual Box Windows 7 x86 1 Гб ОЗУ на базе машины № 1	192.168.1.7	-61
6	клиент-подписчик	Виртуальная машина Virtual Box Windows 7 x86 1 Гб ОЗУ на базе машины № 4	192.168.1.2	-57
7	клиент-подписчик	Нетбук на базе Intel Atom N2800 2c 4t 1.8 ГГц 1Гб 1333 МГц DDR3 под управлением ОС Windows 7 x86	192.168.1.4	-67
8	клиент-подписчик	Одноплатный компьютер Raspberry Pi 3 на базе Broadcom BCM2837 4c 1.2 ГГц 1Гб SDRAM под управлением Raspbian arm64	192.168.1.8	-68

Эксперимент, направленный на определение характера распределения сетевых пакетов внутри системы, длился 3 минуты. Каждые 15 секунд сервер-издатель обновляет данные, а сервер-брокер оповещает об этом связанных с ним клиентов-подписчиков. Каждый клиент-подписчик получает данные из трех различных топиков, соответствующих трем серверам-издателям. Через каждые 2 минуты осуществляется реконфигурация пула доступных мультикаст-групп защищенного обмена данными и каждую минуту участники защищенного обмена данными переподключаются к доступным мультикаст-группам защищенного обмена данными. Сбор статистики принятых и переданных пакетов осуществлялся в трех точках: на сервере-издателе, на сервере-брокере и на клиенте-подписчике. На рис. 4 изображена гистограмма объема переданных и полученных сетевых пакетов в каждой точке.

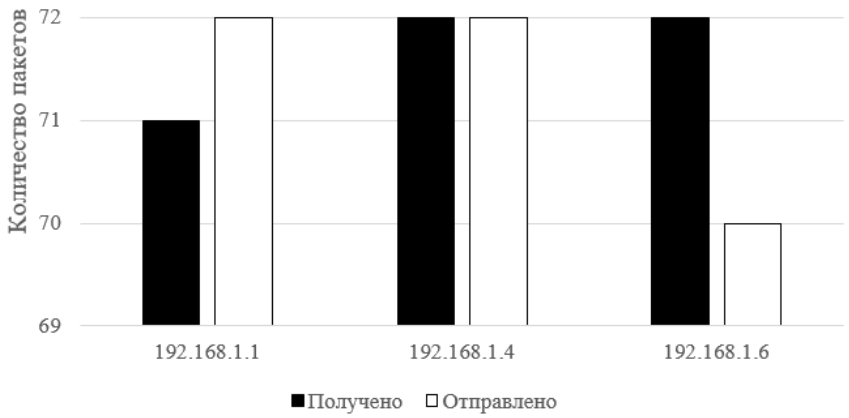

Рис. 4. Объем переданных и полученных пакетов

Сбор данных осуществлялся в течение трех минут. Анализ передаваемых данных осуществлялся в трех точках: сервер-издатель с адресом 192.168.1.1, клиент-подписчик с адресом 192.168.1.4 и сервер-брокер с адресом 192.168.1.6. На рис. 4 изображена гистограмма объема принятого и переданного трафика каждым из трех узлов. Равномерное распределение всего трафика указывает на то, что связь между двумя узлами скрыта среди множества идентичных потоков данных. Злоумышленнику крайне трудно выявить эти связи, а также объем переданных данных между конкретными узлами и их роли в системе.

Тестирование производительности передачи данных осуществлялось по трем параметрам: пропускная способность, задержка и потеря кадров. Размер пакетов одинаков для всех тестов и типов пакетов и составляет 800 байт. Текущая реализация алгоритма выбора мультикаст-групп, который зависит от времени, формирует топологию таким образом, что максимальное расстояние между двумя узлами составляет 2 узла, т.е. пакет максимально ретранслируется дважды, поэтому тестирование проводилось для трех конфигураций:

1) между узлами отсутствуют ретрансляторы;
2) между узлами присутствует 1 ретранслятор;
3) между узлами присутствует 2 ретранслятора.

Пропускная способность измерялась следующим образом: сервер-издатель публикует данные размером 3 Мб на сервере-подписчике, после чего вычисляется скорость передачи информации в зависимости от времени, затраченного на передачу информации, тесты при которых были потери кадров исключаются из эксперимента по определению пропускной способности, но используются при анализе потери кадров. В середину передачи данных вставляется пакет данных, содержащий метку времени отправления данного пакета. Разница между этой временной меткой и временем получения пакета и есть задержка.

Проведено 20 испытаний для каждой конфигурации, где измерялась пропускная способность и задержка, а также анализировалась потеря кадров. В табл. 2 представлены результаты, медианные значения для каждого теста и конфигурации, так как в каждом испытании максимальные и минимальные результаты от медианного отличались незначительно.

Увеличение скорости передачи данных приводит к лавинообразному росту потери кадров, поэтому пропускная способность ограничена максимальными значениями. При значениях, указанных в таблице, отмечались потери кадров в менее чем 10 % испытаний, максимальная потеря составила 3 пакета в испытании при двух ретрансляторах, а минимальная потеря – 1 пакет.

Таблица 2. Характеристики производительности передачи данных

	Без ретрансляторов	Один ретранслятор	Два ретранслятора
Размер пакета (байт)	800	800	800
Пропускная способность (кбит/с)	800	372	166
Пропускная способность (пакет/с)	125	58	26
Задержка (мс)	8	17	38

9. Заключение

По статистике инцидентов информационной безопасности, все больше промышленных предприятий подвергается атакам злоумышленников и многие из этих предприятий не могут им противодействовать. После преодоления сетевого периметра информационной системы злоумышленник осуществляет сетевую разведку. Традиционные меры по обеспечению безопасности локальной вычислительной сети несовершенны и имеют апробированные способы их преодоления. В качестве одной из мер защиты регуляторы предлагают осуществлять сокрытие конфигурации и архитектуры информационной системы, однако в настоящий момент не существует сертифицированных технических средств, реализующих данную меру. Исходя из вышеперечисленного, автором предложен новый метод реализации защищенного обмена данными на основе динамической топологии сети, который в том числе может реализовывать данную меру для сенсорной сети. Кроме того, данный метод передает данные таким образом, при котором скрыты не только данные, но и их источник и получатель, поэтому злоумышленнику потребуются значительные ресурсы, чтобы выявить ценные для себя данные. Характеристики производительности разработанного решения и характер распределения сетевых пакетов показывают, что оно может осуществляться в условиях сенсорной сети для реализации сокрытия её архитектуры и конфигурации и защищенной передачи данных.

Литература

1. Positive Research 2019 [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2019-rus.pdf (дата обращения: 15.03.2020).
2. Positive Research 2018 [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf (дата обращения: 15.03.2020).
3. Infowatch. Утечки данных. Россия. 2016 год [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/reports/17962 (дата обращения: 15.03.2020).
4. *Панасенко А*. Опубликована статистика JSOC по инцидентам ИБ и киберугрозам за 2015 год [Электронный ресурс]. URL: https://www.anti-malware.ru/news/2015-07-09/16455 (дата обращения: 15.03.2020).
5. Перспективный мониторинг. Отчёт Центра мониторинга за второе полугодие 2017 года [Электронный ресурс]. URL: https://www.amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2017-2_amonitoring_halfyear_report.pdf (дата обращения: 15.03.2020).
6. Блог компании Positive Technologies. Статистика появления правил IDS/IPS Suricata для н овых угроз [Электронный ресурс]. URL: https://habr.com/ru/company/pt/blog/282029/ (дата обращения: 15.03.2020).
7. 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.
8. 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.
9. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. 2013. № 136.
10. 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: 16.03.2020).
11. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200103619 (дата обращения: 16.03.2020).
12. ГОСТ Р ИСО/МЭК 27033 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей» [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200089172 (дата обращения: 16.03.2020).
13. 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: 16.03.2020).
14. Payment Card Industry Data Security Standard [Электронный ресурс]. URL: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf (дата обращения: 16.03.2020).
15. NIST SP 800-47 «Security Guide for Interconnecting Information Technology Systems» [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-47.pdf (дата обращения: 16.03.2020).
16. *Germann B., Schmidt M., Stockmayer A., Menth M.* OFFWall: A Static OpenFlow-Based Firewall Bypass // DFN-Forum Kommunikationstechnologien. Günzburg, Germany, 27–28 June 2018. P. 43–55.
17. *Rosenberg I., Gudes E.* Bypassing system calls-based intrusion detection systems. Concurrency and Computation: Practice and Experience. 2017. № 29.
18. *Gu C., Zhang S., Sun Y.* Real-time Encrypted Traffic Identification using Machine Learning // Journal of Software. 2011. V. 6, № 6. P. 1009–1016.
19. *Пескова О. Ю., Халабурда Г. Ю.* Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет // Материалы Всероссийской объединенной конференции «Интернет и современное общество». Санкт- Петербург, 10–12 октября, 2012. С. 348–354.
20. *Abe K., Goto S.* Fingerprinting attack on tor anonymity using deep learning // Proceedings of the Asia-Pacific Advanced Network. Hong-Kong, 31 July – 5 August, 2016. V. 42. P. 15–20.
21. *Egger C., Schlumberger J., Kruegel C., Vigna G.* Practical attacks against the I2P network // Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses. Gros Islet, Saint Lucia, 23–25 October, 2013. P. 432–451.
22. *Zhuang R., DeLoach S.A., Ou X*. Towards a theory of moving target defense // Proceedings of the First ACM Workshop on Moving Target Defense. Scottsdale, Arizona, USA, 3 November, 2014. P. 31–40.

23. *Casola V., De Benedictis A., Albanese M.* A moving target defense approach for protecting resource-constrained distributed devices // 2013 IEEE 14th International Conference on Information Reuse & Integration (IRI). San Francisco, USA, 14–16 August, 2013. P. 22–29.
24. *Dunlop M., Groat S., Urbanski W., Marchany R., Tront J*. MT6D: a moving target ipv6 defense // Military Communications Conference, MILCOM 2011. Baltimore, USA, 7–10 November, 2011. P. 1321–1326.
25. *Kampanakis P., Perros H., Beyene T.* SDN-based solutions for moving target defense network protection // IEEE 15th International Symposium A World of Wireless, Mobile and Multimedia Networks (WoWMoM). Sydney, Australia, 19 June, 2014. P. 1–6.
26. *Hunkeler U., Truong H. L., Stanford-Clark A.* MQTT-S – A publish/subscribe protocol for wireless sensor networks. // 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08). Bangalore, India, 6–10 January, 2008. P. 791–798.

Статья поступила в редакцию 06.05.2020.

Кушко Евгений Александрович
аспирант кафедры безопасности информационных технологий, СибГУ им. М. Ф. Решетнева (660037, Красноярск, просп. им. газеты Красноярский рабочий, 31), тел. (391) 2-621-847, e-mail: evgeny.kushko@gmail.com.

Secure data communication implementing method based on dynamic network topology

E. Kushko

This study deals with countering interception and analysis of network traffic. The paper covers statistics of information security incidents related to hacker attacks on enterprise information systems, analyses regulatory requirements for ensuring secure data communication over the network and network security in general, and compares existing solutions for ensuring secure data communication and countering unauthorized interception and analysis of network traffic as well as solutions providing concealment of the information system structure and configuration. A new method for secure data communication based on dynamic network topology is presented. This method differs from the existing solutions by hiding the participants of the network interaction. Practical implementation of the method was carried out for hiding architecture and configuration of the sensor network.

Keywords: local network, secure data communication, data transfer protocol, moving target defense technology.