DOI: 10.55648/1998-6920-2023-17-4-62-73 УДК 123.456.789

# Организация защищенного обмена данными внутри программно-управляемой локальной сети *

Е. А. Кушко, Н. Ю. Паротькин, В. В. Золотарев

Сибирский университет науки и технологий (Красноярск)

*Аннотация*: **Введение.** Для обеспечения защищенного обмена данными внутри локальной вычислительной сети информационной системы недостаточно защиты лишь внешнего периметра. Данный факт подтверждается аналитическими отчетами ведущих компаний в области информационной безопасности. Как правило, после преодоления внешнего сетевого периметра перед проведением атаки злоумышленник выполняет действия по сетевой разведке. Успех выполнения сетевой атаки зависит от полноты собранной информации. Постоянные изменения топологии сети не позволяют злоумышленнику обладать долгосрочной информацией о ней, в результате чего он вынужден более интенсивно собирать информацию, тем самым выдав себя. В противном случае эффективность планируемой атаки снижается. Целью данного исследования является повышение защищенности сторон внутрисетевого обмена методом динамической реконфигурации топологии сети. Авторами предложено новое решение для обеспечения безопасного взаимодействия узлов в сети от внутреннего и преодолевшего защиту сетевого периметра внешнего злоумышленника.

**Материалы и методы.** Предлагаемое решение построено на базе программно-управляемой сети и технологии VxLAN. Решение предполагает постоянную реконфигурацию сети как с определенной периодичностью, так и по наступлении определенных событий, чтобы злоумышленник не мог обладать долгосрочной информацией о ней. В случае, если злоумышленник был обнаружен или возник инцидент информационной безопасности, сеть в автоматическом режиме реконфигурируется так, чтобы минимизировать или исключить возможные последствия.

**Результаты.** Полученные результаты экспериментов по применению предлагаемого решения показывают, что периодические изменения топологии сети не позволяют злоумышленнику собрать полную информацию о сети в скрытом режиме. В результате работы предлагаемого решения он может быть обнаружен, а также изолирован.

**Обсуждение и заключение.** Предлагаемое решение показало потенциальную применимость для организации защищенного обмена данными внутри локальной вычислительной сети информационной системы.

*Ключевые слова*: программно-управляемая сеть, технология защиты движущейся цели, безопасность обмена данными, защита от исследования, защищенная передача данных.

*Для цитирования*: Кушко Е. А., Паротькин Н. Ю., Золотарев В. В. Организация защищенного обмена внутри программно-управляемой локальной сети // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 62–73. https://doi.org/10.55648/1998-6920-2023-17-4-62-73.



Статья поступила в редакцию 05.04.2023;
принята к публикации 07.06.2023.

* Данное исследование выполнено при финансовой поддержке Минцифры РФ (Грант ИБ). Проект №40469-07/2021-К.

## 1. Введение

Несмотря на наличие защиты внешнего сетевого периметра информационной системы, злоумышленники находят недостатки и уязвимости в ней – компания Positive Technologies в своей аналитике [1] приводит следующую статистику:

- в рамках внешнего тестирования на проникновение различных компаний в 92 % случаев был получен доступ к их локальной вычислительной сети;
- в 100 % случаев злоумышленник может подключиться к корпоративным беспроводным сетям;
- в 63 % систем через беспроводные сети получен доступ к ресурсам локальных вычислительных сетей.

Для решения этой проблемы исследовательские группы разрабатывают системы автоматизации сбора, мониторинга и анализа событий информационной безопасности с целью выявления инцидентов информационной безопасности и последующего реагирования на них. Но существует также и другой подход, появившийся относительно недавно, а именно технология Moving-Target Defense (MTD, технология защиты от движущейся цели) [2].

Как правило, после проникновения в локальную сеть информационной системы злоумышленник выполняет следующие действия [3]:

1) закрепление в системе;
2) сбор информации;
3) изучение окружения;
4) построение топологии сети;
5) сканирование портов;
6) идентификация узлов, сервисов и операционных систем;
7) определение ролей узлов;
8) поиск уязвимостей;
9) определение вектора атаки и её реализация.

Это также подтверждается статистикой инцидентов информационной безопасности:

1) компания Positive Technologies отмечает, что в 33 % компаний наблюдалось сканирование внутренней сети, а в 19 % – сбор информации [1];

2) компания Ростелеком Солар также в своем отчете указывает на то, что после проникновения в сеть злоумышленник выполняет её сканирование [4];

3) компания Kaspersky ICS CERT установила, что APT-группировки используют инструменты для сканирования и кражи данных [5].

Для обеспечения безопасности сети технология защиты движущейся цели предполагает периодические изменения информации о конечной точке (IP, MAC, используемые порты) и маршрутах передачи данных. Технология защиты движущейся цели обычно не предполагает активного противодействия злоумышленнику, но при этом не позволяет ему обладать актуальной информацией о сети, на основе которой он принимает решения при реализации своей атаки. В результате, не осуществив этап сетевой разведки и, следовательно, не получив нужную информацию, злоумышленник не может эффективно осуществить атаку [6].

## 2. Сравнение с существующими решениями и методами защиты

Традиционно для защиты передаваемых данных от перехвата используют построение эшелонированной системы защиты, а для защиты от анализа – шифрование. В случае, если злоумышленник преодолел один или несколько эшелонов защиты, он очень часто ничем не ограничен, что косвенно подтверждает приведенная ранее статистика (данные собраны в организациях, которые имели систему защиты информации). Шифрование защищает данные от анализа, однако перехват даже зашифрованных пакетов позволяет получить злоумышленнику некоторые полезные данные [7].

В настоящий момент решения технологии защиты движущейся цели для локальных вычислительных сетей имеют ряд существенных недостатков:

1) неконтролируемый рост энтропии, ухудшающий производительность системы [8];

2) разрывы связи между легитимными пользователями и объектами защиты [9];

3) невозможность использовать в устаревшей сетевой инфраструктуре [10];

4) недостаточный уровень исследования применения технологии для реальных сетей и высокое разнообразие тестовых сред, которое затрудняет сравнение различных методов и стратегий друг с другом [11].

Большинство недостатков текущих реализаций связано с попыткой исследователей и разработчиков защитить всю сеть при помощи технологии движущейся цели. В своем решении авторы предполагают защитить не всю сеть, а лишь её часть, предназначенную для обмена критичными данными.

К аналогичным предлагаемому авторами решению с точки зрения активного противодействия злоумышленнику относятся решения из класса систем Security Orchestration, Automation and Response (SOAR, платформы оркестрации, автоматизации и реагирования на инциденты безопасности). Решения данного класса предполагают реконфигурирование сети и информационной системы таким образом, чтобы злоумышленник в случае его обнаружения был немедленно изолирован. В результате работы решений данного класса часто возникают ошибки первого рода [12], из-за которых доступ к легитимным сервисам в сети может быть нарушен. Соответственно, в результате применения предлагаемого авторами решения на базе коммуникационного оборудования будет создано дополнительное буферное время. Это позволит снизить вероятность ошибки первого рода за счет дополнительного времени для сигнализации и анализа информации, поступающей от средств защиты, а сам злоумышленник будет переведен на этап изучения окружения.

В настоящее время широко применяемыми решениями проблемы защиты от исследования являются следующие технологии: deep packet inspection (DPI), брокер сетевых пакетов, virtual private network (VPN), software-defined network (SDN), стегоканал.

Технология DPI предназначена для анализа трафика в режиме реального времени, включая уровень приложений модели OSI. Сетевой трафик, в зависимости от заданных правил, может быть заблокирован, перенаправлен, модифицирован, ограничен по скорости и т.д. Решения из класса DPI также позволяют обнаружить вредоносный трафик. Производительность напрямую зависит от аппаратной платформы, причем данная технология предполагает кластеризацию. Решения DPI имеют распределенную структуру: сервер и сенсоры. В случае, если устройство DPI подключается «в разрыв», могут возникнуть проблемы с передачей данных. Также устройство DPI может быть интегрировано с другими средствами защиты информации [13].

Брокеры сетевых пакетов, в отличие от средств DPI, прежде всего направлены на распределение и балансировку сетевого трафика с учетом требований целостности сессий. Фильтрация трафика осуществляется до транспортного уровня включительно. Основная цель фильтрации – повышение надежности сеть и эффективности анализа сетевого трафика: балансировка нагрузки, детуннелирование, из заголовков пакетов удаляются избыточные данные, удаление повторяющихся пакетов, дешифрация пакетов, сбор статистики проходящего трафика и т.д. Кроме того, брокеры сетевых пакетов предлагают функционал по маскированию сетевых пакетов с целью анонимизации трафика. Производительность также зависит от аппаратной платформы. Брокеры сетевых пакетов могут быть интегрированы с другими средствами защиты информации [14].

VPN переводится как виртуальная частная сеть. VPN – это оверлейная сеть, которая предназначена для защищенной передачи данных через публичные сети. Пользователь подключается к шлюзу, через который осуществляется подключение к внутренней сети. Данные шифруются только при передаче по небезопасному каналу. Требования к вычислительным ресурсам зависят от количества клиентов. Некоторые VPN-протоколы поддерживают сокрытие метаданных соединения [15].

SDN – это сеть передачи данных, управление которой осуществляется программно, в том числе и в режиме реального времени. SDN предназначена для централизованного управления всей сетью, чтобы оперативно конфигурировать сеть и реагировать на изменения в сети, оптимизировать передачу трафика, упрощать процесс конфигурирования, централизованно применять политики и т.д. Управляющие пакеты данных могут быть зашифрованы. Управление осуществляется централизованно. Специальных требований к вычислительным ресурсам у данной технологии нет [16].

Еще одним решением, которое может быть применено для защиты от исследования, является стегоканал. Стегоканал – это канал передачи сообщений, в котором данные кодируются методами стеганографии. В случае передачи данных по сети, как правило, данные скрываются в заголовках и полях полезной нагрузки сетевых пакетов, также применяется модификация последовательности передачи данных. Дополнительно применяется шифрование для защиты передаваемых данных. Однако объем данных, который можно передать средствами сетевой стеганографии, существенно ограничен [17].

Для сравнения предлагаемого решения (табл. 1) с ранее упомянутыми технологиями выбраны следующие критерии:

1) возможная пропускная способность канала;
2) наличие возможности изменения правил управления каналом в режиме реального времени;
3) требуемая вычислительная мощность решения;
4) наличие шифрования;
5) наличие сокрытия метаданных соединения;
6) система управления каналом – децентрализованная, частично централизованная, централизованная;
7) наличие возможности работы в качестве источника событий для SIEM;
8) негативное влияние на стабильность работы всей сети и конечных узлов;
9) сложность технологии.

Таблица 1. Сравнение с существующими решениями

| Крит. | DPI | Брокер сетевых пакетов | VPN | SDN | Стегоканал | Предлагаемое решение |
|---|---|---|---|---|---|---|
| 1 | Высокая | Высокая | Высокая | Высокая | Низкая | Высокая |
| 2 | Да | Да | Нет | Да | Нет | Да |
| 3 | Высокая | Высокая | Средняя | Низкая | Низкая | Низкая |
| 4 | Нет | Нет | Да | Нет | Да | Да |
| 5 | Нет | Да | Да | Нет | Да | Да |
| 6 | Центр. | Центр. | Центр. | Центр. | Децентр. | Центр. |
| 7 | Да | Да | Да | Нет | Нет | Да |
| 8 | Да | Нет | Нет | Да | Нет | Да |
| 9 | Высокая | Высокая | Высокая | Средняя | Средняя | Средняя |

## 3. Описание предлагаемого решения

Предлагаемое авторами решение сочетает в себе два подхода:

1) постоянные изменения структуры сети, в результате чего актуальность собранных злоумышленником данных имеет малое время жизни;

2) в случае обнаружения злоумышленника сеть реконфигурируется таким образом, что злоумышленник будет изолирован от остальной сети.

В основе решения лежат принципы сети SDN, в которой узлы имеют доступ к ней и её ресурсам строго в соответствии с определенными политиками, которые задаются админи-

стратором программными средствами централизованно и применяются на каждом устройстве сети от единой точки управления [18].

Решение построено на базе технологии Virtual Extensible Local Area Network (VxLAN, виртуальная расширенная частная сеть). Каждый узел подключен как минимум к двум виртуальным сетям, одна из которых является базовой для всех узлов, обеспечивающих выполнение базового сетевого взаимодействия и обмена открытой информацией, а другие сети – для организации защищенного обмена данными. Выбор технологии VxLAN обусловлен его преимуществами относительно других аналогичных технологий: масштабируемость, гибкость, эффективность, простота конфигурации и управления [19].

Технология VxLAN, как правило, применяется для разделения потоков передачи данных в рамках одной физической среды, например, для центров обработки данных [20], IoT-решений (Internet of Things, интернет вещей) [21], систем мобильной связи [22]. Исследования безопасности VxLAN показывают, что данная технология действительно обеспечивает изоляцию оверлейных сетей, имеет устойчивость к распространенным атакам, и её недостатки могут быть исправлены правильным конфигурированием сетевого оборудования, а также использованием средств обнаружения вторжений [23].

Решение предполагает постоянное реконфигурирование сети, т.е. перемещение узлов по виртуальным сетям по наступлении некоторых событий:

1) по истечении некоторого временного интервала, чтобы злоумышленник не мог обладать актуальной информацией о всей сети;

2) в результате обнаружения злоумышленника для его изоляции;

3) в результате возникновения некоторого инцидента для предотвращения или минимизации его последствий.

## 4. Описание экспериментов

Для практического исследования данного решения была собрана одноранговая сеть в среде виртуальной лаборатории EVE-NG (рис. 1). Узел, который обозначен на рисунке как «Nmap», осуществляет сканирование сети соответствующей утилитой. Узел, обозначенный как «Snort», является контроллером сети, на котором развернуто соответствующее средство обнаружения вторжений. Остальные узлы образуют инфраструктуру сети. Все узлы подключены к виртуальному коммутатору под управлением операционной системы Cisco NX-OS.

Конфигурирование осуществляется следующим образом. Каждый узел подключен к двум виртуальным сетям: одна сеть предназначена для взаимодействия с контроллером сети, а другая – для организации защищенного обмена данными. Контроллер сети сообщает узлам по запросу VLAN ID и параметры виртуальной сети, к которой необходимо подключиться на следующей итерации реконфигурирования. Данный идентификатор сопоставляется сетевым оборудованием с VxLAN Network Identifier (VNI, сетевой идентификатор VxLAN) виртуальной сети и гарантирует соответствие инфраструктуры конфигурации контроллера.

При наступлении следующей итерации реконфигурирования сети контроллер настраивает сетевое оборудование таким образом, чтобы каждый узел был подключен к той виртуальной сети и имел доступ к тем сетевым ресурсам, которые определены политикой контроллера. В случае, если был обнаружен узел сети, скомпрометированный злоумышленником, контроллер конфигурирует сеть так, чтобы этот узел был изолирован от остальной инфраструктуры. Правила обнаружения заданы таким образом, чтобы обнаруживать сканирование Nmap [24], что моделирует худший вариант реализации системы защиты для злоумышленника.

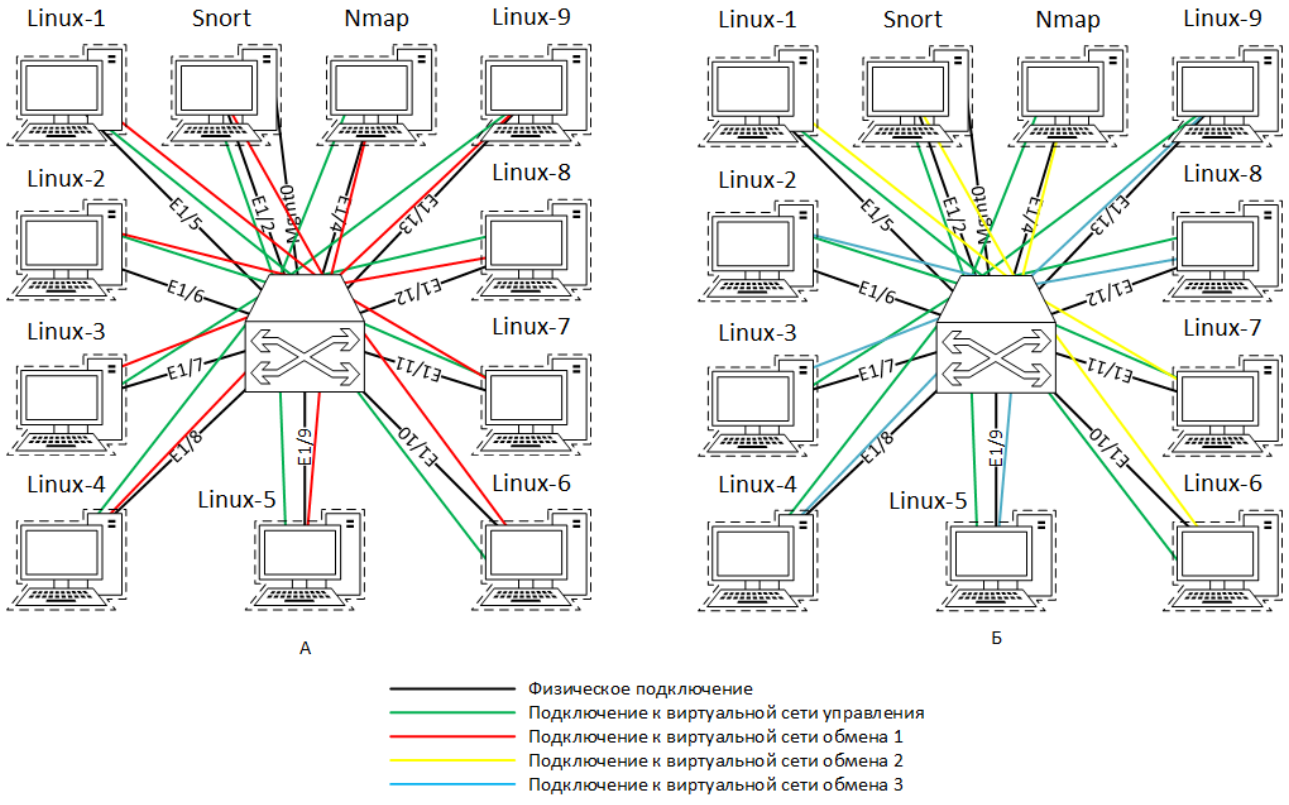


Рис. 1. Конфигурация сети: А – до реконфигурации, Б – после реконфигурации по таймеру

Взаимодействие узлов построено на основе протокола JSON-RPC 2.0 [25] over HTTP(s) для конфигурирования контроллером сетевого оборудования (NX-API) и JSON-RPC 2.0 over WebSocket для взаимодействия узлов (клиентов) с контроллером (сервером).

## 5. Результаты

Эксперимент построен на двух типах сканирования (табл. 2): безумный (5 – insane) и хитрый (1 – sneaky), а также проведен для трех типов триггеров реконфигурирования [26]:

1) без реагирования;

2) истечение временного интервала;

3) возникновение инцидента информационной безопасности, в данном случае – обнаружение сканирования.

Эксперимент необходим для получения количественной оценки результата анализа защищаемой сети злоумышленником.

Таблица 2. Результаты эксперимента

| Тип сканирования | Без реагирования | Истечение временного интервала 60 с | Обнаружение сканирования |
|---|---|---|---|
| Безумный (Insane) | Сканирование завершено за 305.16 с | Прервано на 11.04 % (сканирование портов) | Прервано на 0.76 % (сканирование портов) |
| Хитрый (Sneaky) | Сканирование завершено за 1478.77 с | Прервано на 20.20 % (обнаружение хостов) | Прервано на 0.76 % (сканирование портов) |

Также была осуществлена оценка потерь при переконфигурации сети. Первый эксперимент был проведен при помощи утилиты ping. Опрос осуществлялся в течение одной минуты

с интервалом в 1 секунду, размер пакета – 64 байта. Через 10 секунд после начала эксперимента инициировалась реконфигурация сети. В первом эксперименте происходит потеря не более чем 18 пакетов icmp (в худшем случае) и 10 пакетов icmp (в среднем) при взаимодействии через защищенную сеть между любыми двумя узлами. Второй эксперимент был проведен при помощи утилиты iperf. На скорости 1 Мбит/с в течение одной минуты генерировался синтетический udp-трафик, а через 10 секунд после начала эксперимента инициировалась реконфигурация сети. Были использованы различные размеры пакетов: 64, 128, 256, 512, 1024, 1280 и 1518 байт. Во втором эксперименте, вне зависимости от размера пакета, наблюдалась потеря 50 % пакетов (в среднем) и 51 % (в худшем случае). Стоит отметить, что без переконфигурации сети потерь нет. Для каждого эксперимента проведено не менее чем 10 испытаний. Использовалась виртуальная сеть EVE-NG с максимальной пропускной способностью 1 Гбит/с. Другой трафик в сети отсутствовал.

На основе результатов эксперимента можно сделать вывод о том, что реконфигурации необходимо осуществлять по оповещениям от средств защиты информации, и в случае, если есть подозрение на то, что злоумышленник все-таки преодолел внешний сетевой периметр, а также скомпрометировал некоторый узел и успешно избежал свое обнаружение, необходимо реконфигурировать сеть через интервалы времени, при которых злоумышленник не сможет обладать долгосрочной информацией, не выдав себя, осуществляя более интенсивный сбор данных.

## 6. Заключение

Из статистики инцидентов информационной безопасности очевидно, что защиты внешнего сетевого периметра недостаточно. После проникновения в сеть злоумышленник обычно осуществляет сетевую разведку – это, как правило, один из ключевых этапов реализации сетевой атаки. В качестве меры защиты, как правило, используют сбор, анализ и мониторинг событий информационной безопасности для выявления инцидентов и реагирования на них.

Также данную проблему можно решить при помощи другого подхода – технологии защиты движущейся цели, которая заключается в постоянных изменениях в сети, при котором злоумышленник не может обладать долгосрочной информацией о ней и в результате не сможет эффективно осуществить свою атаку. Такое решение авторами было представлено при изменении информационной топологии сети с использованием multicast-групп в беспроводной среде с высоким риском перехвата пакетов, но обладающее ограниченной областью применения для работы в сенсорных сетях [27].

В данной работе авторами предложено решение, которое объединяет оба подхода: с одной стороны, сеть реконфигурируется по истечении временного интервала, а с другой – по оповещениям средств защиты информации. В случае обнаружения злоумышленника сеть реконфигурируется таким образом, что злоумышленник изолируется от остальной сети. Данное решение построено на принципах SDN и технологии VxLAN с сохранением функциональных характеристик сети.

Предлагаемое решение может являться частью SOAR-системы, то есть средством автоматической реакции на действия злоумышленника, приводящим систему в базовое состояние, в котором злоумышленнику требуется начинать реализацию атаки сначала.

## Литература

1. Positive Research 2020 [Электронный ресурс]. URL: `https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf` (дата обращения: 04.04.2023).

2. *Lei C., Zhang, H., Tan J., Zhang, Y., and Liu X.* Moving target defense techniques: A survey // Security and Communication Networks. 2018. V. 2018.
3. *Galtsev A. A., Sukhov A. M.* Network attack detection at flow level // Smart Spaces and Next Generation Wired/Wireless Networking. Springer, Berlin, Heidelberg, 2011. P. 326 –334.
4. Solar JSOC Security Report 2020 [Электронный ресурс]. URL: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf (дата обращения: 04.04.2023).
5. 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: 04.04.2023).
6. *Sengupta S., Chowdhary A., Sabur A., Alshamrani A., Huang D., and Kambhampati S.* A survey of moving target defenses for network security // IEEE Communications Surveys and Tutorials. 2020. V. 22, № 3. P. 1909–1941.
7. *Velan P., Čermák M., Čeleda P., and Drašar M.* A survey of methods for encrypted traffic classification and analysis // International Journal of Network Management. 2015. V. 25, № 5. P. 355–374.
8. *DeLoach S., Ou X., Zhuang R, and Zhang S.* Model-driven, moving-target defense for enterprise network security // Models@ run. time. 2014. P. 137–161.
9. *Cho J., Sharma D., Alavizadeh H., Yoon S., Ben-Asher N., Moore T., Kim D., Lim H., and Nelson F.* Toward proactive, adaptive defense: A survey on moving target defense // IEEE Communications Surveys and Tutorials. 2020. V. 22, № 1. P. 709–745.
10. *Xu X., Hu H., Liu Y., Zhang H., and Chang D.* An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector // Security and Communication Networks. 2021. V. 2021.
11. *Jalowski Ł., Zmuda M., Rawski M.* A Survey on Moving Target Defense for Networks: A Practical View // Electronics. 2022. V. 11, № 18.
12. *Mir A., Ramachandran R.* Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems // Proc. 6th International Conference on Intelligent Computing and Applications. Singapore, 2021. V. 3. P. 157–169.
13. *Кошепаров Д. Я.* Программная реализация систем глубокой проверки пакетов // Вестник науки и образования. 2020. № 12-1 (90). С. 21–25.
14. Современные решения для построения систем информационной безопасности – брокеры сетевых пакетов (Network Packet Broker) [Электронный ресурс]. URL: https://habr.com/ru/company/dsol/blog/490252/ (дата обращения: 04.04.2023).
15. *Ezra P., Misra S., Agrawal A., Oluranti J., Maskeliunas R., and Damasevicius R.* Secured communication using virtual private network (VPN) // Proc. International Conference on Cyber Security and Digital Forensics (ICCSDF), 2021. P. 309-319.
16. *Goransson P., Black C., Culver T.* Software defined networks: a comprehensive approach. Morgan Kaufmann, 2016.
17. *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.
18. *Shin S., Xu L., Hong S., and Gu G.* Enhancing network security through software defined networking (SDN) // Proc. 25th International conference on computer communication and networks (ICCCN), Waikoloa, HI, USA, 2016. P. 1–9.
19. *Shahrokhkhani V.* An Analysis on Network Virtualization Protocols and Technologies [Электронный ресурс]. URL: https://era.library.ualberta.ca/items/2c481b73-7ebf-4a51-b6e9-ff5b1224fada/view/f0cd1ea5-7314-4e12-a85a-99e76022195a/Shahrokhkhani.pdf (дата обращения: 04.04.2023).

20. *Pu H., Wang Y., An X.* Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology // Journal of Computer and Communications. 2020. V. 8, № 8. P. 45–58.
21. *Shif L., Wang F., Lung C.* Improvement of security and scalability for IoT network using SD-VPN // Proc. IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 2018. P. 1–5.
22. *Gu R., Zhang X., Yu L., and Zhang J.* Enhancing Security and Scalability in Software Defined LTE Core Networks // Proc. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, USA, 2018. P. 837–842.
23. *Reyes G., Dammers M., Kastanja M.* Security assessment on a VXLAN-based network // Haettu. 2014. V. 10, № 2017. P. 2013–2014.
24. *Liao S., Zhou C., Zhao Y., Zhang Z., Zhang C., Gao Y., and Zhong G.* A Comprehensive detection approach of Nmap: principles, rules and experiments // Proc. International conference on cyber-enabled distributed computing and knowledge discovery (CyberC), Chongqing, China, 2020. P. 64–71.
25. JSON-RPC Working Group. JSON-RPC 2.0 Specification [Электронный ресурс]. URL: `https://www.jsonrpc.org/specification` (дата обращения: 04.04.2023).
26. *Jetty S.* Network Scanning Cookbook: Practical Network Security Using Nmap and Nessus 7. Packt Publishing Ltd, 2018.
27. *Кушко Е. А.* Метод реализации защищенного обмена данными на основе динамической топологии сети // Вестник СибГУТИ. 2020. № 4 (52). С. 39–52.

**Кушко Евгений Александрович**
старший преподаватель кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва, e-mail: `evgeny.kushko@gmail.com`, ORCID ID: 0000-0003-1290-7075.

**Паротькин Николай Юрьевич**
к.т.н., доцент кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва, e-mail: `ny-parotkin@yandex.ru`, ORCID ID: 0000-0002-3486-0602.

**Золотарев Вячеслав Владимирович**
к.т.н., заведующий кафедрой безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнёва (СибГУ, 660037, Красноярск, пр. имени газеты «Красноярский рабочий», д. 31), тел. +7 391 222 7639, e-mail: `amida.2@yandex.ru`, ORCID ID: 0000-0002-8054-8564.

*Авторы прочитали и одобрили окончательный вариант рукописи.*
*Авторы заявляют об отсутствии конфликта интересов.*
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

**Ensuring Secure Data Exchange in Software-defined Local Network**

Evgenii A. Kushko, Nikolai Yu. Parotkin, Vyacheslav V. Zolotarev

Reshetnev Siberian State University of Science and Technology

*Abstract*: **Introduction.** Protecting outer perimeter is not enough to ensure secure data communication in the information system of local area network. Analytical reports of leading information security companies confirm this fact. Usually, an attacker having overcome the outer perimeter conducts network reconnaissance before carrying out an attack. The success of a network attack depends on the completeness of the information collected. The constantly changing network topology does not provide an attacker with long-term network topology information, as a result, the attacker is forced to collect information more intensively thereby identifying himself. Otherwise, the effectiveness of the planned attack is reduced. The aim of this research is to increase the intra-network data transfer security level by means of network topology dynamic reconfiguration. The authors proposed a new solution for ensuring secure node interaction countering both internal and external attackers having overcome an outer perimeter.
**Materials and methods.** The proposed solution is based on a software-defined network and VxLAN technology. The solution involves constant network reconfiguration both with a certain frequency and on the occurrence of certain events, so that an attacker could not have long-term information. If an intruder is detected or an information security incident occurs, the network is automatically reconfigured in such a way as to lessen or prevent possible consequences.
**Results.** The obtained results show that periodic network changes do not allow an attacker to covertly collect complete information about the network, and the proposed solution may allow to detect and isolate the attacker.
**Discussion and conclusion.** The obtained results show that it is possible to apply the proposed solution for organizing secure data communication within the local computer network of the information system.

*Keywords*: software-defined network, moving target defense, data exchange security, network scanning protection, secure data communication.

*For citation*: Kushko E. A., Parotkin N. Yu., Zolotarev V. V. Ensuring secure data exchange in software-defined local network (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 1, pp. 62-73. https://doi.org/10.55648/1998-6920-2023-17-4-62-73.



The article was submitted: 05.04.2023;
accepted for publication 07.06.2023.

## References

1. Positive Research 2020, available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2020-rus.pdf (accessed: 04.04.2023).
2. Lei C., Zhang, H., Tan J., Zhang, Y., Liu X. Moving target defense techniques: A survey, *Security and Communication Networks*. 2018, vol. 2018.
3. Galtsev A. A., Sukhov A. M. Network attack detection at flow level. *Smart Spaces and Next Generation Wired/Wireless Networking*, Springer, Berlin, Heidelberg, 2011, pp. 326 - 334.
4. Rostelecom Solar. Solar JSOC Security Report 2020, available at: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf (accessed: 04.04.2023).
5. Kaspersky ICS CERT. APT-ataki na promyshlennye kompanii v 2020 godu [APT attacks on industrial companies in 2020], available at: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-companies-in-2020-Ru.pdf (accessed: 04.04.2023).
6. Sengupta S., Chowdhary A., Sabur A., Alshamrani A., Huang D., and Kambhampati S. A survey of moving target defenses for network security. *IEEE Communications Surveys and Tutorials,* 2020, vol. 22, no. 3, pp. 1909-1941.
7. Velan P., Čermák M., Čeleda P., and Drašar M. A survey of methods for encrypted traffic classification and analysis. *International Journal of Network Management*, 2015, vol. 25, no. 5, pp. 355-374.
8. DeLoach S., Ou X., Zhuang R, and Zhang S. Model-driven, moving-target defense for enterprise network security. *Models@ run. Time*, 2014, pp. 137-161.

9. Cho J., Sharma D., Alavizadeh H., Yoon S., Ben-Asher N., Moore T., Kim D., Lim H., and Nelson F. Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys and Tutorials*, 2020, vol. 22, no. 1, pp. 709-745.
10. Xu X., Hu H., Liu Y., Zhang H., and Chang D. An Adaptive IP Hopping Approach for Moving Target Defense Using a Light-Weight CNN Detector. *Security and Communication Networks*, 2021, vol. 2021.
11. Jalowski Ł., Zmuda M., Rawski M. A Survey on Moving Target Defense for Networks: A Practical View. *Electronics*, 2022, vol. 11, no. 18.
12. Mir A., Ramachandran R. Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems. *6th International Conference on Intelligent Computing and Applications*, Singapore, 2021, vol. 3, pp. 157-169.
13. Kosheparov D. Ya. Programmnaya realizaciya sistem glubokoj proverki paketov [Software implementation of deep packet inspection systems]. *Vestnik nauki i obrazovaniya*, 2020, no. 12-1(90), pp. 21-25.
14. Sovremennye resheniya dlya postroeniya sistem informacionnoj bezopasnosti – brokery setevyh paketov (Network Packet Broker) [Modern solutions for building information security systems - network packet brokers], available at: `https://habr.com/ru/company/dsol/blog/490252/` (accessed: 04.04.2023).
15. Ezra P., Misra S., Agrawal A., Oluranti J., Maskeliunas R., and Damasevicius R. Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, 2022, pp. 309-319.
16. Goransson P., Black C., Culver T. *Software defined networks: a comprehensive approach*. Morgan Kaufmann. 2016.
17. Peskova O. Yu., Halaburda G. Yu. *Primenenie setevoj steganografii dlya zashchity dannyh, peredavaemyh po otkrytym kanalam Internet* [Application of network steganography for protection of the data transferred over the internet]. *Materialy Vserossijskoj ob"edinennoj konferencii «Internet i sovremennoe obshchestvo»*, 2012, pp. 348-354.
18. Shin S., Xu L., Hong S., and Gu G. Enhancing network security through software defined networking (SDN). *2016 25th international conference on computer communication and networks (ICCCN)*, Waikoloa, HI, USA, 2016, pp. 1-9.
19. Shahrokhkhani V. An Analysis on Network Virtualization Protocols and Technologies, available at: `https://era.library.ualberta.ca/items/2c481b73-7ebf-4a51-b6e9-ff5b1224fada/view/f0cd1ea5-7314-4e12-a85a-99e76022195a/Shahrokhkhani.pdf` (accessed: 04.04.2023).
20. Pu H., Wang Y., An X. Safety Protection Design of Virtual Machine Drift Flow in Cloud Data Center Based on VXLAN Technology. *Journal of Computer and Communications*, 2020, vol. 8, no. 8, pp. 45-58.
21. Shif L., Wang F. Lung C. Improvement of security and scalability for IoT network using SD-VPN. *2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, Taiwan, 2018, pp. 1-5.
22. Gu R., Zhang X., Yu L., and Zhang J. Enhancing Security and Scalability in Software Defined LTE Core Networks. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE),* New York, USA, 2018, pp. 837-842.
23. Reyes G., Dammers M., Kastanja M. Security assessment on a VXLAN-based network. *Haettu*, 2014, vol. 10, no. 2017, pp. 2013–2014.
24. Liao S., Zhou C., Zhao Y., Zhang Z., Zhang C., Gao Y., and Zhong, G. A Comprehensive detection approach of Nmap: principles, rules and experiments. *2020 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*, Chongqing, China, 2020, pp. 64–71.
25. JSON-RPC Working Group. JSON-RPC 2.0 Specification, available at: `https://www.jsonrpc.org/specification` (accessed: 04.04.2023).
26. Jetty S. *Network Scanning Cookbook: Practical Network Security Using Nmap and Nessus 7*. Packt Publishing Ltd. 2018.
27. Kushko.E. A. *Metod realizacii zashchishchennogo obmena dannymi na osnove dinamicheskoj topologii seti* [Secure data communication implementing method based on dynamic network topology]. Vestnik SibGUTI, 2020, no. 4(52), pp. 39-52.

**Evgenii A. Kushko**
Senior lecturer of the department of information technologies security, Reshetnev Siberian State University of Science and Technology (660037, Russia, Krasnoyarsk, Imeni gazety «Krasnoyarskiy rabochiy» pr. 31), phone: +7 391 222 7639, e-mail: evgeny.kushko@gmail.com, ORCID ID: 0000-0003-1290-7075.

**Nikolay Yu. Parotkin**
Cand. of Sci. (Engineering), assistant professor of the department of information technologies security, Reshetnev Siberian State University of Science and Technology, e-mail: nyparotkin@yandex.ru, ORCID ID: 0000-0002-3486-0602.

**Vyacheslav V. Zolotarev**
Cand. of Sci. (Engineering), head of department of information technologies security, Reshetnev Siberian State University of Science and Technology, e-mail: amida.2@yandex.ru, ORCID ID: 0000-0002-8054-8564.