Защита информации в интеллектуальных транспортных системах управления городским транспортом

Information security in intelligent mass transit management systems

Алексеев В.М.[1]*, Чичков С.Н.[1]
Victor M. Alekseev[1]*, Sergey N. Chichkov[1]
[1]*Российский университет транспорта (МИИТ), Москва, Российская Федерация*
[1]*Russian University of Transport (MIIT), Moscow, Russian Federation*
**alekseevvm@rambler.ru*


Алексеев В.М.


Чичков С.Н.

Резюме. Цель. *В данной статье рассматриваются вопросы формирования архитектуры и требования к архитектуре сетей передачи данных при создании интеллектуальной системы управления городской транспортной системой.* **Методы.** *В статье предлагается архитектура сети с использованием технологии меток мультисервисной сети MPLS, маршрутизации информационных потоков. Реализация ядра локальной вычислительной сети с использованием полносвязности позволяет по меткам информационных потоков заранее сформировать маршруты обмена информации между серверами и приложениями информационно-телекоммуникационной сети (ИТС). Применение технологии мультисервисных сетей с метками (MPLS) является базой для построения сети управления и сбора информации в ИТС. Это позволяет унифицировать технические решения по подключению подсистем, выполняющих различные функции в ИТС, например, управления и диагностики, с минимальными задержками доставлять информацию до серверов управления и отправлять ответственные команды управления, а также унифицировать подключение датчиков – контроллеров через интерфейс Ethernet или беспроводные интерфейсы 4G и 5G.* **Выводы.** *Реализация принципа сборки и разборки маршрутов информационных потоков для критически важных объектов значительно усложняет проведение атак и организацию сбора информации о сетевой структуре ИТС.*

Abstract. Aim. *The paper examines matters related to the definition of the architecture and requirements for data communication networks as part of intelligent mass transit management systems.* **Methods.** *The paper suggests a network architecture using multiprotocol label switching (MPLS) technology and traffic routing. If the core of a local area network is implemented using fully-connected topology, the use of flow labels allows predefining information exchange routes between servers and applications of an information and telecommunications network (ITS). Multiprotocol label switching (MPLS) is the foundation of control and information acquisition networks of ITS. That allows adopting common interfaces to the subsystems that perform various functions within an ITS, e.g., control and diagnostics, minimizing the time of information delivery to management servers and sending critical control commands, as well as using common Ethernet or 4G/5G wireless interfaces.* **Conclusions.** *The path installation/removal principle, when applied to critical facilities, significantly complicates attacks and collection of information on the network structure of ITS.*

Ключевые слова: *информационный поток, мультисервисная сеть, интерфейс, локальные сети, интеллектуальные транспортные системы, протокол, доверенный маршрут.*
Keywords: *information flow, multiservice network, interface, local area networks, intelligent transportation systems, protocol, trusted path.*

Для цитирования: *Алексеев В.М., Чичков С.Н. Защита информации в интеллектуальных транспортных системах управления городским транспортом // Надежность. 2022. №3. С. 62-68. https://doi.org/10.21683/1729-2646-2022-22-3-62-68*
For citation: *Alekseev V.M., Chichkov S.N. Information security in intelligent mass transit management systems. Dependability 2022;3: 62-68. https://doi.org/10.21683/1729-2646-2022-22-3-62-68*

Поступила *24.04.2022 г.* / **После доработки** *10.05.2022 г.* / **К печати** *19.09.2022 г.*
Received on: *24.04.2022* / **Revised on:** *10.05.2022* / **For printing:** *19.09.2022.*

Создание защиты информационных систем является одним из важнейших направлений. Однако необходимо создавать системы защиты таким образом, чтобы они не были пост-фиксирующими появления атак, а направлены были на предотвращение их проведения. Иными словами, модели должны быть построены таким образом, чтобы они не дали возможность противнику, даже при проникновении на некоторые объекты, получить необходимую информацию. Известно, что в операционные системы встроены тайные агенты сбора и передачи информации. Для их старта достаточно, чтобы была передана команда извне на инициализацию скрытого канала передачи информации. При использовании скрытых каналов передача происходит без изменений параметров информационных потоков. Но для обеспечения передачи необходима интеграция информационных потоков на объектах локальной сети. Тайные агенты с использованием комбинаторики выстраивают последовательности пакетов в заранее определенные комбинации, определяющие начало, конец, комбинацию нулей или единиц. Это позволяет, последовательно, без изменения объемов предаваемой информации, осуществлять передачу информации.

Необходимо отметить, что организация скрытого канала возможна при наличии в информационном потоке нескольких разнотипных пакетов (с различными протоколами в DATA в пакете Ethernet), например тремя или четырьмя. Рекомендации ведущих компаний по организации локальных сетей направлены на построение именно таких сетей, где интеграция потоков максимально присутствует. Система очередей, построенная на использовании стека, также способствует организации скрытой передачи информации, так как позволяет формировать требуемые комбинации путем посылки из стека необходимого типа пакета. Предотвратить организацию скрытых каналов возможно с использованием интеллектуальной модели формирования информационных потоков.

Как это происходит. Первое условие реализации модели – это применение полносвязности объектов. Второе условие – использование принципов изолированной программной среды, позволяющей разделить информационные потоки.

Суть полносвязности в обеспечении защиты состоит в том, что маршруты могут быть организованы по различным объектам сети. Отсюда вытекает, что информационный поток может проходить через различные объекты (в различные моменты времени), что вызывает затруднения атакующего противника, поскольку он не может заранее знать маршрут информационного потока. При этом маршрут, использованный ранее для реализации информационного потока, разбирается, и собирается новый маршрут.

Изолированная программная среда предполагает использование в сети технологии виртуализации VLAN, что позволяет информационным потокам быть корректными, то есть не воздействовать на соседние информационные потоки. Включение в пакет идентификатора VLAN и порта обеспечивает необходимую маршрутизацию потоков в информационной системе. Реализация модели формирования маршрутов основана на использовании многорядного перцептрона. Эта модель реализуется на базе сервера мониторинга безопасности объектов (МБО).

Рассмотрим работу модели МБО. Одной из актуальных задач в области информационной безопасности в системах интеллектуального управления является мониторинг безопасности объектов, который должен обеспечивать формирование доверенных маршрутов и отслеживание информационных потоков, контроль подключений внешних объектов или субъектов, конфигурирование маршрутизаторов и взаимодействие с коммутаторами. Для объектов транспорта эта задача на порядок важнее, поскольку транспорт относится к критически важным сферам функционирования отраслей экономики и должен обеспечивать безопасную перевозку пассажиров и грузов. Исходя из этого, основная задача МБО состоит в контроле подключений к критически важным объектам инфраструктуры предприятия и управлении доверенными маршрутами сети в режиме реального времени, что позволит своевременно реагировать и предотвращать несанкционированные действия внешних пользователей, и, как следствие, исключить возможность хищения данных, а также нарушения работоспособности серверов. Решение поставленной задачи возможно при использовании теоретических положений, в основе которых лежит использование принципа полносвязности [1]. В работе рассматриваются вопросы практической реализации теоретических положений, направленных на построение модели формирования доверенных маршрутов (сборки и разборки) с целью предотвращения утечки данных за счет быстрой перенастройки маршрутов для информационных потоков. На рис. 1 приведена структура сети, наиболее часто используемой для реализации систем интеллектуального управления, состоящая из мультисервисной сети MPLS [2], объединяющей множество распределенных объектов систем автоматики и связи, энергообеспечения и инфраструктуры движения транспортных средств. В сети центра находятся серверы систем управления подвижными (TRAIN APP), стационарными объектами (ELECTRO APP, APP CTRL) и другим оборудованием. Дополнительно в сеть центра введено ядро из коммутаторов, на которых происходит формирование доверенных маршрутов (сервер МБО) для информационных потоков ИТС. Включение ядра коммутаторов (вместо одного центрального) позволяет организовать сборку и разборку маршрутов, что делает невозможным внедрение тайного агента сбора информации в центральном коммутаторе, если бы использовался рекомендуемый вариант интеграции потоков через центральный коммутатор с маршрутизацией. В интеллектуальных системах для доставки приоритетных пакетов требуется минимальная по времени задержка, для чего необходимо выбрать кратчайший маршрут, содержащий минимальное количество промежуточных

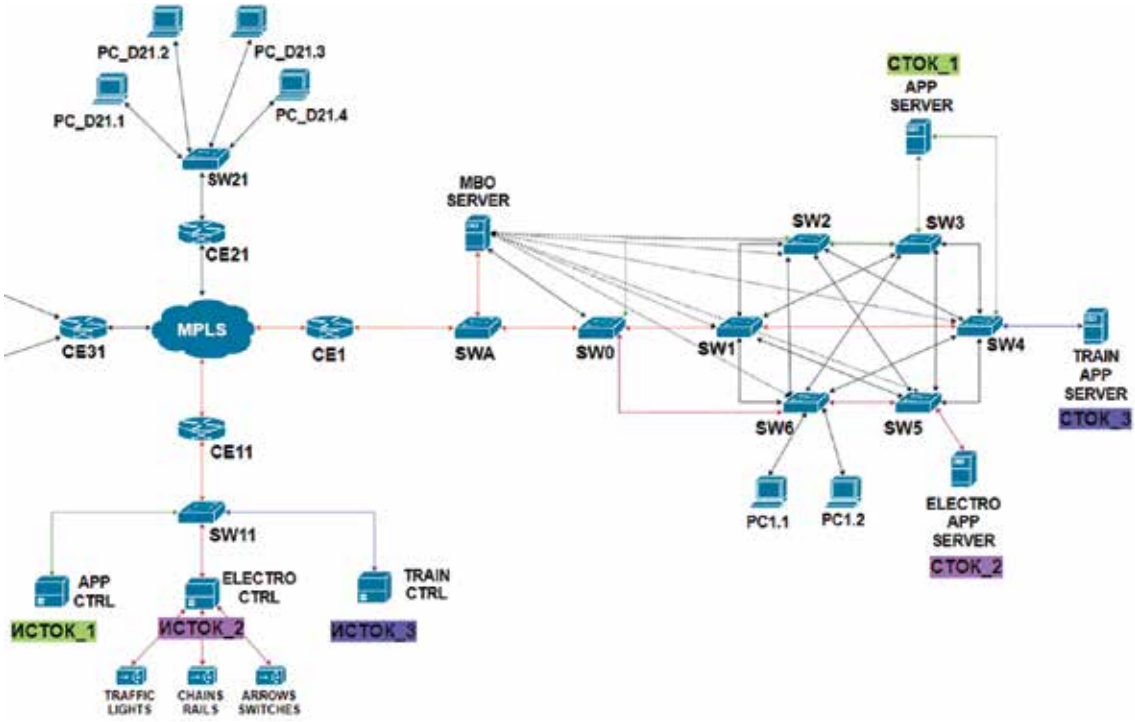

Рис. 1. Структура сети транспортной системы

объектов. Наиболее загруженным является информационный поток APP CTRL, так как в нем осуществляется передача команд управления и контроля за состоянием устройств автоматики, обеспечивающих безопасность перевозок. В этой связи, для информационного потока APP CTRL необходимо будет использовать дополнительные маршруты доставки информации, что повысит объемы передаваемой информации.

Рассчитывает и формирует маршруты сервер МБО (рис. 1). Для построения маршрутов используется модель многорядного перцептрона [3, 4]. Изображение ядра сети представлено на рис. 2.

Опишем процесс формирования маршрутов. Начинаем прокладывать маршрут от истоков к стокам. В нашем ядре присутствует три пары информационных потоков «исток-сток». Для данной топологии следует рассчитывать первый, второй ряд перцептрона. На первом ряду получаем кратчайшие маршруты, на втором ряду дополнительные, включающие один промежуточный маршрут. Выбираем вид опорной функции, с помощью которой будем отбирать кратчайшие маршруты и строить критерий. Ввиду того, что требуется выполнить операцию декартового произведения, функция будет иметь вид [3, 4]:

$$O[SW_i^{is^m}]\times O[SW_j^{st^m}];i\neq j;i,j=1,n. \qquad (1)$$

На первом ряду перцептрона будут декартовы произведения пар, входящих в ядро, с метками $is^1, st^1, is^2, st^2, is^3, st^3$, а также объектов без меток. Критерий отбора кратчайшего маршрута $kr^{(1)}$ на первом ряду (индекс 1) для каждой пары имеет вид:

$$kr^{(1)}=O[SW_i^{is^m}]\times O[SW_j^{st^m}];i\neq j;i,j=1,n\,. \qquad (2)$$

В критерии присутствуют метки $is^1, st^1, is^2, st^2, is^3, st^3$, между которыми мы должны найти кратчайшие маршруты в полносвязной сети. В данном случае это маршруты между объектами с метками $is^m->st^m, m=1,3$. Второй ряд перцептрона формируется из декартовых произведений, не отобранных в первом ряду, как кратчайший маршрут. В этой связи, критерий (индекс 2) отбора дополнительных маршрутов имеет вид:

$$kr^{(2)}=O[SW_i^{is^m}]*O[SW_5]*O[SW_j^{st^m}];$$

$$s\neq i,j;i\neq j;i,j=1,n;is^m->st^m,m=1,3\,.$$

Далее выполним построение всех маршрутов, применив декартово произведение к объектам ядра сети с группировкой:

$$O[SW_1^{is^{1.1}},e1_{SW2\text{-}e0}]\times O[SW_2^{is^1},e0_{SW1\text{-}e1}]+O[SW_1^{is^{1.1}},e2_{SW3\text{-}e1}]\times$$
$$\times O[SW_3^{st^1},e1_{SW1\text{-}e2}]+O[SW_1^{is^{1.1}},e3_{SW4\text{-}e2}]\times O[SW_4^{st^{1.1}},e2_{SW1\text{-}e3}]+$$
$$+O[SW_1^{is^{1.1}},e4_{SW5\text{-}e1}]\times O[SW_5,e1_{SW1\text{-}e4}]+O[SW_1^{is^{1.1}},e5_{SW6\text{-}e1}]\times$$
$$\times O[SW_6^{is^1},e1_{SW1\text{-}e5}]+O[SW_2^{is^1},e7_{SW6\text{-}e2}]\times O[SW_6^{is^1},e2_{SW2\text{-}e7}]+$$
$$+O[SW_2^{is^1},e6_{SW5\text{-}e2}]\times O[SW_5,e2_{SW2\text{-}e6}]+O[SW_2^{is^1},e5_{SW4\text{-}e3}]\times$$
$$\times O[SW_4^{st^{1.1}},e3_{SW2\text{-}e5}]+O[SW_2^{is^1},e4_{SW3\text{-}e0}]\times O[SW_3^{st^1},e0_{SW2\text{-}e4}]+$$
$$+O[SW_3^{st^1},e3_{SW6\text{-}e3}]\times O[SW_6^{is^1},e3_{SW3\text{-}e3}]+O[SW_3^{st^1},e2_{SW5\text{-}e3}]\times$$
$$\times O[SW_5,e3_{SW3\text{-}e2}]+O[SW_3^{st^1},e1_{SW4\text{-}e4}]\times O[SW_4^{st^{1.1}},e4_{SW3\text{-}e1}]+$$
$$+O[SW_4^{st^{1.1}},e1_{SW6\text{-}e4}]\times O[SW_6,e4_{SW4\text{-}e1}]+O[SW_4^{st^{1.1}},e0_{SW5\text{-}e4}]\times$$
$$\times O[SW_5,e4_{SW4\text{-}e0}]+O[SW_5,e0_{SW6\text{-}e5}]\times O[SW_6^{is^1},e5_{SW5\text{-}e0}], \qquad (3)$$

где *ei* – интерфейсы коммутаторов.

Выполним построение маршрутов для информационного потока APP STRL ИСТОК_1(is^1) – СТОК_1(st^1) основного и дополнительного ИСТОК_1.1($is^{1.1}$) – СТОК_1.1($st^{1.1}$). В связи с тем, что сервер приложения (APP STRL) имеет два интерфейса подключения к двум разным коммутаторам (рис. 1) необходимо рассмотреть дополнительный маршрут.

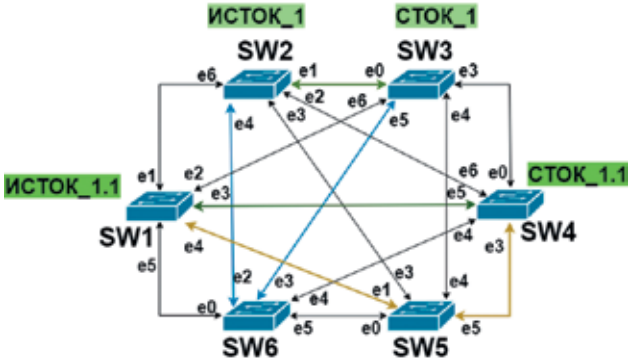

Рис. 2. Маршруты для информационного потока APP STRL ИСТОК_1(is^1) – СТОК_1(st^1) и ИСТОК_1.1($is^{1.1}$) – СТОК_1.1($st^{1.1}$)

Согласно топологии сети на рис. 2, может быть несколько маршрутов для информационного потока APP CTRL. Рассмотрим формирование кратчайшего и дополнительных маршрутов. Пусть ИСТОК_1 => $O[SW2]$, ИСТОК_1.1 => $O[SW1]$, а соответственно СТОК_1 => $O[SW3]$, СТОК_1.1 => $O[SW4]$. Рассмотрим построение маршрута ИСТОК_1(is^1) – СТОК_1(st^1). Поиск маршрута потока осуществляем по меткам, свидетельствующим о подключении интерфейса объекта ядра к потоку приложения (APP STRL):

- маршрут 1 – $O[SW_1^{is^1}, e2_{SW3\text{-}e1}] \times O[SW_3^{st^1}, e1_{SW1\text{-}e2}]$;
- маршрут 2 – $O[SW_1^{is^1}, e3_{SW4\text{-}e2}] \times O[SW_4^{st^1}, e2_{SW1\text{-}e3}]$;
- маршрут 3 – $O[SW_2^{is^1}, e5_{SW4\text{-}e3}] \times O[SW_4^{st^1}, e3_{SW2\text{-}e5}]$;
- маршрут 4 – $O[SW_2^{is^1}, e4_{SW3\text{-}e0}] \times O[SW_3^{st^1}, e0_{SW2\text{-}e4}]$.

Из всех вышеперечисленных маршрутов на первом ряду перцептрона подходит маршрут 4. Маршрут кратчайший и отвечает поставленному критерию. Следовательно, отбираем этот маршрут в пул решений для потока ИСТОК_1 – СТОК_1, при условии включения этого информационного потока через порты коммутаторов SW_2 и SW_3, посредством прописки VLANi на их портах (VLANi соответствует заданному информационному потоку APP CTRL).

Для вычисления дополнительного маршрута между ИСТОК_1 – СТОК_1 находим декартово произведение из произведений, содержащих метки is^1, st^1, которые поступают на второй ряд перцептрона. Остальные члены уравнения (3) для поиска дополнительного маршрута исключаем. Отбор осуществляем по критерию:

$$O[SW_i^{is^1}, e4_{SW3\text{-}e0}] \times O[SW_5, e2_{SW2\text{-}e4}, e3_{SW3\text{-}e5}] \times O[SW_j^{st^1}, e0_{SW2\text{-}e4}];$$

$s \neq i, j; i \neq j; i, j = 1, n$.

Ниже приведены возможные дополнительные маршруты ИСТОК_1 – СТОК_1:

- маршрут 1 – $O[SW_2^{is^1}, e4_{SW3\text{-}e0}] \times O[SW_6, e2_{SW2\text{-}e4}, e3_{SW3\text{-}e5}] \times O[SW_3^{st^1}, e0_{SW2\text{-}e4}]$;
- маршрут 2 – $O[SW_2^{is^1}, e4_{SW5\text{-}e3}] \times O[SW_5, e3_{SW2\text{-}e4}, e4_{SW3\text{-}e4}] \times O[SW_3^{st^1}, e4_{SW6\text{-}e4}]$;
- маршрут 3 – $O[SW_2^{is^1}, e2_{SW4\text{-}e6}] \times O[SW_4, e6_{SW2\text{-}e2}, e0_{SW3\text{-}e3}] \times O[SW_3^{st^1}, e3_{SW4\text{-}e0}]$;
- маршрут 4 – $O[SW_2^{is^1}, e6_{SW1\text{-}e1}] \times O[SW_1, e1_{SW2\text{-}e6}, e2_{SW3\text{-}e6}] \times O[SW_3^{st^1}, e6_{SW3\text{-}e2}]$.

За дополнительный маршрут могут быть приняты маршруты 1, 2, 3, 4.

Во втором ряду перцептрона формируется резервная маршрутизация для увеличения пропускной способности информационного потока через ядро. Рассмотрим пару ИСТОК_1.1 => $O[SW_1^{is^{1.1}}]$ – СТОК_1.1 => $O[SW_4^{st^{1.1}}]$, как дополнительные маршруты для APP CTRL. Эта необходимость обусловлена большой величиной информационного потока, приоритетностью передачи команд управления и контроля. Из уравнения (3) получаем кратчайший маршрут, соответствующий поставленному критерию:

маршрут 2 – $O[SW_1^{is^{1.1}}, e3_{SW4\text{-}e2}] \times O[SW_4^{st^{1.1}}, e2_{SW1\text{-}e3}]$.

Для получения дополнительных маршрутов на втором ряду перцептрона, перемножим объекты с метками $is^{1.1}$, $st^{1.1}$, получаем возможные маршруты:

- маршрут 1 – $O[SW_1^{is^{1.1}}, e1_{SW2\text{-}e6}] \times O[SW_2, e6_{SW1\text{-}e1}, e2_{SW4\text{-}e6}] \times O[SW_4^{st^{1.1}}, e6_{SW2\text{-}e2}]$;
- маршрут 2 – $O[SW_1^{is^{1.1}}, e2_{SW3\text{-}e6}] \times O[SW_3, e6_{SW1\text{-}e2}, e3_{SW4\text{-}e0}] \times O[SW_4^{st^{1.1}}, e0_{SW3\text{-}e3}]$;
- маршрут 3 – $O[SW_1^{is^{1.1}}, e4_{SW5\text{-}e1}] \times O[SW_5, e1_{SW1\text{-}e4}, e5_{SW4\text{-}e3}] \times O[SW_4^{st^{1.1}}, e3_{SW5\text{-}e5}]$;
- маршрут 4 – $O[SW_1^{is^{1.1}}, e5_{SW6\text{-}e0}] \times O[SW_6, e0_{SW1\text{-}e5}, e4_{SW4\text{-}e4}] \times O[SW_4^{st^{1.1}}, e4_{SW6\text{-}e4}]$. (4)

Отбор маршрутов в (4) осуществлен по критерию: $O[SW_i^{is^{1.1}}, e4_{SW3\text{-}e0}] \times O[SW_5, e2_{SW2\text{-}e4}, e3_{SW3\text{-}e5}] \times O[SW_j^{st^{1.1}}, e0_{SW2\text{-}e4}]$; $s \neq i, j; i \neq j; i, j = 1, n$. В качестве дополнительного маршрута может быть выбран любой из перечисленных выше.

Рассмотрим формирование маршрута для информационного потока ELECTRO APP, пометив вход и выход ИСТОК_2 – СТОК_2. Находим декартово произведение всех объектов, присвоив объектам метки: исток ИСТОК_2 => $SW_6^{is^2}$ и сток СТОК_2 => объект $SW_5^{st^2}$. Отобранный кратчайший маршрут для информационного потока с метками is^2, st^2, подходящий к ИСТОК_2 => $SW_6^{is^2}$ и выходящий через

СТОК_2 => объект $SW_5^{st^2}$, имеет вид $O[SW_6^{is^2}, e5_{SW5\text{-}e0}] \times O[SW_5^{st^2}, e0_{SW6\text{-}e5}]$. Формирование дополнительных маршрутов для потока с метками is^2, st^2 дает следующий результат $O[SW_6^{is^2}, e3_{SW3\text{-}e5}] \times O[SW_5, e5_{SW1\text{-}e3}, e4_{SW5\text{-}e4}] \times O[SW_5^{st^2}, e4_{SW3\text{-}e4}]$; $s \neq i, j; i \neq j; i, j = 1, n$. Определим маршрут для информационного потока (TRAIN CTRL) ИСТОК_3 => $O[SW1]$ – СТОК_3 => $O[SW4]$. Кратчайший маршрут имеет вид: $O[SW_1^{is^3}, e3_{SW4\text{-}e2}] \times O[SW_4^{st^3}, e2_{SW1\text{-}e3}]$. Находим дополнительные маршруты, получаем:

$O[SW_1^{is^3}, e4_{SW5\text{-}e1}] \times O[SW_5, e1_{SW1\text{-}e4}, e5_{SW4\text{-}e3}] \times O[SW_4^{st^3}, e3_{SW5\text{-}e5}]$; $s \neq i, j; i \neq j; i, j = 1, n$.

Конфигурирование сети начинается с определения количества коммутаторов составляющих ядро, далее мы формируем полносвязную сеть – устанавливаем связь каждого с каждым через порты коммутаторов *ei* ядра SW_5ei. В нашей сети заранее известны информационные потоки: APP CTRL, ELECTRO CTRL, TRAIN CTRL. После подключения, мы смотрим на топологию сети, чтобы понимать на какой из коммутаторов у нас приходит изначально информационный поток и с какого выходит, то есть «ИСТОК-СТОК».

После формирования в модели маршрутов на МБО, конфигурируем их в нашем ядре, состоящем из коммутаторов. Конфигурация производится не на отдельный интерфейс, а на подинтерфейс, для расширения количества маршрутов, это возможно при использовании технологии инкапсуляции (dot1Q), которая предусмотрена производителем сетевых аппаратных устройств – «Cisco» [5, 6, 7, 8, 9]. Каждому подинтерфейсу присваивается VLAN метка маршрута (метки инкапсулируются на порты VLAN), например, если выбран *k* маршрут из всех возможных *N*, $k \in N$, номер метки VLAN примет значение *k*. Новое подключение будет работать строго по этому маршруту, как только клиент разорвет соединение, сервер МБО сменит маршрут на другое из *N* номеров, исключая предыдущий из списка выбора и применит к следующему новому клиенту сети. Конфигурирование коммутатора Cisco с добавлением 12 VLAN выглядит следующим образом:

enable – включаем консоль;

configure terminal – заходим в конфигуратор;

interface FastEthernet0/3.k – выбираем интерфейс для конфигурирования, номер порта – 3;

encapsulation dot1Q k – задаем инкапсуляцию по протоколу dot1Q и значение метки VLAN = k;

no shutdown – производим включение интерфейса;

exit – выходим из конфигуратора;

copy running – config startup – config – сохраняем нововведения на коммутаторе в энергонезависимую память.

После настройки каждого коммутатора автоматически прокладываются маршруты и по ним можно передвигаться. Что касается ограничений на входе в ядро сети, там предусмотрен маршрутизатор, который соединяет напрямую клиента с сервером МБО; после валидной верификации проверки пароля подключения сервер МБО с помощью протокола удаленного доступа SSH выполняет отправку конфигурационного файла, который в свою очередь применяет необходимый VLAN на подключенного клиента, сам конфигурационный файл для отправки выглядит следующим образом:

enable – включаем консоль;

configure terminal – заходим в конфигуратор;

interface FastEthernet0/1 – выбираем интерфейс для конфигурирования и номер порта;

switchport mode access – включаем доступ для порта;

switchport access VLAN k – записываем значения VLAN;

no shutdown – производим включение интерфейса;

exit – выходим из конфигуратора;

copy running – config startup – config – сохраняем информацию на коммутаторе в энергонезависимую память.

После этого клиент проходит по маршруту, указанному сервером МБО, а когда клиент разрывает подключение к сети, сервер МБО формирует снова конфигурационный файл, но уже с другим маршрутом. Таким образом, цель реализации состоит в обеспечении невозможности отслеживания в компьютерной системе информационных потоков. Это обеспечивается посредством использования полносвязного ядра, позволяющего формировать систему динамических доверенных маршрутов для внешних и внутренних пользователей. Принцип работы анализатора и сети направлен на дезориентирование злоумышленника в понимании топологии корпоративной сети. Применение данного алгоритма позволяет добиться повышенной защищенности сети.

Оценим повышение информационной безопасности при реализации предложенного метода. Задано: полносвязная сеть из *n* объектов. Исток из объекта $i \in n$, сток $k \in n$. Маршруты простые $M = n \times (n-1)/2 - 1$.

Задача противника *z* получить доступ к объекту, по которому может вероятно проходить маршрут, с целью завладения информацией. Стратегия защиты, то есть модель формирования маршрутов, противнику неизвестна. Ввиду простоты маршрутов информационный поток проходит по объектам без повторов.

Рассмотрим первый случай. Противник проникает на один объект. Вероятность захвата противником объекта 1 и наличия действующего маршрута $m \in M$ из *n* равна (исходя из условия независимости событий [10]:

$$P^1_{m \cup z} = 1 - (1 - P^1_{m \in M}) \times (1 - P^1_z),$$

где $P^1_{m \in M}$ – вероятность прохождения простого маршрута *m* через объект 1;

P^1_z – вероятность овладения доступом объекта 1 противником *z*;

$m \cup z$ – знак вероятности пересечения двух независимых событий: маршрут *m* проходит по 1 объекту, захваченному противником *z*.

Рассмотрим случай второй. Противник z проникает на два объекта 1 и 2. Вероятность захвата противником двух объектов 1 и 2 и наличия действующего маршрута $m \in M$ на одном из этих объектов $<1,2> \in n$ равна:

$$P^{1,2}_{m \bigcup z} = 1 - [(1 - P^1_{m \in M}) \times (1 - P^1_z)] \times [(1 - P^2_{m \in M}) \times (1 - P^2_z)],$$

где $P^{1,2}_z$ – вероятность овладения доступом объекта 1 и 2 противником z.

Величины $(1 - P^1_z)$ и $(1 - P^2_z)$ определяют вероятности не захвата противником z объектов 1 и 2. Принимаем $P^1_z \neq P^2_z$ (так как может во многом зависеть от объекта, например точка доступа или маршрутизатор), а $P^1_{m \in M} = P^2_{m \in M}$.

$(1 - P^1_{m \in M}), (1 - P^2_{m \in M})$ – вероятности отсутствия маршрута на объектах 1 или 2, определяются $P^1_{m \in M}$ при $n >> <1,2> (1 - P^1_{m \in M}) - > 1, (1 - P^2_{m \in M}) - > 1$.

Определим вероятность прохождения маршрута $m \in M$ через один из объектов полносвязной сети

$$P^{1,2}_{m \in M} = 1! * (n - l)! / n! \qquad (5)$$

В формуле (5) объекты сток и исток исключаем из рассмотрения в предположении невозможности захвата их противником z. Таким образом, из n исключены два (l=2) объекта. Рассмотрим вариант организации локальной сети без использования полносвязности, то есть стандартным способом. Вероятность прохождения маршрута через объект и если объект взят под контроль противником z (совпадение двух независимых событий), определяется:

$$P^1_{m \bigcup z} = 1 - (1 - P^1_{m \in M}) \times (1 - P^1_z),$$

где $P^1_{m \in M} = 1$, что приводит к вероятности получения информации противником z $P^1_{m \bigcup z} = 1$. В случае изменения конфигурации локальной сети и добавления объекта вероятность будет равна $P^1_{m \in M} = 0,5$. Принимаем вероятность проникновения на один объект, равную P^1_z, определим значение $P^1_{m \bigcup z}$ для стандартного случая и случая с полносвязной сетью, имеем:

$P^1_{m \bigcup z} = 1 - (1 - 0,5) \times (1 - P^1_z)$ – для стандартного подключения;

$P^1_{m \bigcup z} = 1 - (1 - 0,08) \times (1 - P^1_z)$ – полносвязной сети n=10, l=2.

Из приведенного выше следует, что защищенность объектов многократно повышается при использовании полносвязной сети и принципов изолированной программной среды.

Заключение. Цель реализации состоит в построении защиты информации с применением интеллектуального принципа «опережения». Это обеспечивается посредством использования полносвязного ядра, позволяющего формировать систему динамических доверенных маршрутов для внешних и внутренних пользователей, а также перцептрона для формирования маршрутов и случайного их выбора (сервер МБО).

Принцип работы анализатора и сети направлен на дезориентирование противника в понимании топологии корпоративной сети, поскольку происходит постоянное изменение маршрутов информационных потоков.

Реализована технология конфигурирования маршрутов внутри ядра сети, подробно описана рассматриваемая сеть с отображением интерфейсов подключений.

Благодарности. Исследование выполнено при финансовой поддержке РФФИ, НТУ «Сириус», ОАО «РЖД» и Образовательного Фонда «Талант и успех» в рамках научного проекта № 20-37-51001.

Библиографический список

1. Kharitonova E.V. Graphs and networks. Ulyanovsk: UlSTU, 2006. 92 p.

2. Thomas Nadeau. MPLS Network Management MIBs, Tools, and Techniques. Morgan Kaufmann Publishers, 2002. 525 p.

3. Alekseev V.M., Baranov L.A., Sidorenko V.G., Kulagin M.A. название???? // World of transport, Vol. 19, No. 1 (92) 2021. Pp. 18-46.

4. Ivakhnenko A.G. Longterm forecasting and management of complex systems. Kiev, Technics, 1975. 310 p.

5. Devyanin P.N. Computer systems security models. M.: Hotline-Telecom, 2018. 338 p.

6. Dave Klein. Relying on firewalls? Here's why you'll be hacked // Network Security. Volume 2021. Issue 1. January 2021. Pp. 9-12.

7. Sudhir Udipi. The event data management problem: getting the most from network detection and response // Network Security. Volume 2021. Issue 1. January 2021. Pp. 12-14.

8. Michael Wood. How SASE is defining the future of network security // Network Security. Volume 2020**.** Issue 12. December 2020. Pp. 6-8.

9. Jan Harrington. Network Security A Practical Approach. Morgan Kaufmann Publishers, 2005. 384 p.

10. Вентцель Е.С. Теория вероятностей. М.: ГИФМЛ, 1962. 564 с.

References

1. Kharitonova E.V. Graphs and networks. Ulyanovsk: UlSTU; 2006. (in Russ.)

2. Nadeau T. MPLS Network Management MIBs, Tools, and Techniques. Morgan Kaufmann Publishers; 2002.

3. Alexeev V.M., Baranov L.A., Sidorenko V.G., Kulagin M.A. Building Architecture of Intelligent Control System for Urban Rail Transit System. *World of transport and transportation* 2021;1(92):18-46.

4. Ivakhnenko A.G. Longterm forecasting and management of complex systems. Technics; 1975. (in Russ.)

5. Devyanin P.N. Computer systems security models. Moscow: Hotline-Telecom; 2018. (in Russ.)

6. Klein D. Relying on firewalls? Here's why you'll be hacked. *Network Security* 2021;1:9-12.

7. Udipi S. The event data management problem: getting the most from network detection and response. *Network Security* 2021;1:12-14.

8. Wood M. How SASE is defining the future of network security. *Network Security* 2020;12:6-8.

9. Harrington J. Network Security. A Practical Approach. Morgan Kaufmann Publishers; 2005.

10. Wentzel E.S. Probability theory. Moscow: GIFML; 1962. (in Russ.)

Сведения об авторах

Алексеев Виктор Михайлович – доктор технических наук, профессор, профессор кафедры «Управление и защита информации», Российский университет транспорта (МИИТ), Москва, Российская Федерация, e-mail: alekseevvm@rambler.ru.

Чичков Сергей Николаевич – аспирант кафедры «Управление и защита информации», ассистент кафедры «Высшая математика», Российский университет транспорта (МИИТ), Москва, Российская Федерация, e-mail: seriozha.tchichkov@yandex.ru.

About the authors

Victor M. Alekseev, Doctor of Engineering, Professor, Professor of the Department of Management and Protection of Information, Russian University of Transport (MIIT), Moscow, Russian Federation, e-mail: alekseevvm@rambler.ru.

Sergey N. Chichkov, post-graduate student, Department of Management and Protection of Information, Russian University of Transport (MIIT), Moscow, Russian Federation, e-mail: seriozha.tchichkov@yandex.ru.

Вклад авторов в статью

Алексеев В.М. Разработка архитектуры сети с использованием технологии меток мультисервисной сети MPLS, маршрутизации информационных потоков. Предложение применения модели реализации ядра локальной вычислительной сети с использованием полносвязности.

Чичков С.Н. Обзор и анализ существующего состояния рассматриваемой проблемы. Исследование литературных источников и интернет-изданий, оформление статьи.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.