ДВУХУРОВНЕВАЯ СТРУКТУРА ПОСТРОЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ ПОЛНОСВЯЗНОСТИ

Научная статья

Алексеев В.М.[1, *], Хусенов Д.Н.[2], Чичков С.Н.[3]
[2] ORCID : 0009-0003-4178-6935;
[1, 2, 3] Российский университет транспорта (МИИТ), Москва, Российская Федерация

* Корреспондирующий автор (alekseevvm[at]rambler.ru)

Аннотация

В статье рассматривается метод построения локальной инфраструктуры с использованием полносвязности. Особенность предлагаемого решения заключается в том, что функционально сеть разделена на два уровня. Первый уровень подключается к сети интернет. На этом уровне расположены защитные ресурсы, а именно различные анализаторы информационных потоков, осуществляющие анализ трафика, поступающего из сети интернет в корпоративную сеть, и предотвращающие атаки из внешней сети. Во втором уровне расположены ресурсы — персональные компьютеры, серверы и другие сетевые объекты. Второй уровень, как и первый, использует полносвязную сеть, и все объекты подключаются интерфейсами к полносвязной сети.

Применение предложенной структуры построения сети позволяет анализировать входящий в корпоративную сеть и предотвращать различные компьютерные атаки, в частности, различные виды DDoS атак, атаки перехвата трафика, атаки на web-приложения, например, SQL- и XSS-инъекции.

Второй уровень полносвязной сети, который направлен на анализ внутренних потоков в корпоративной сети, где минимизируются случаи заражения рабочих мест пользователей компании и других устройств корпоративной сети вирусными программами.

Целью данной работы является реализация двухуровневой структуры сети, построенной на принципах полносвязности.

Задачами являются разработка модели функционирования первого и второго уровней полносвязной сети, а также модели формирования маршрутов в предлагаемой структуре и защита от внутренних и внешних атак.

В статье используются теория и методы графов, а также метод группового учета аргументов.

Ключевые слова: информационный поток, корпоративная сеть, интеллектуальные транспортные системы, доверенный маршрут, доверенный процесс, анализатор трафика, полносвязная сеть.

TWO-LEVEL STRUCTURE OF BUILDING INFORMATION PROTECTION IN A CORPORATE NETWORK ON THE BASIS OF FULL CONNECTIVITY

Research article

Alekseev V.M.[1, *], Khusenov D.N.[2], Chichkov S.N.[3]
[2] ORCID : 0009-0003-4178-6935;
[1, 2, 3] Russian University of Transport (MIIT), Moscow, Russian Federation

* Corresponding author (alekseevvm[at]rambler.ru)

Abstract

The article examines the method of building a local infrastructure using full connectivity. The distinctive feature of the proposed solution is that the network is functionally divided into two levels. The first level is connected to the Internet. At this level are located security resources, namely various information flow analysers that perform analysis of traffic coming from the Internet to the corporate network and prevent attacks from the external network. The second layer contains resources – personal computers, servers and other network objects. The second layer, like the first layer, uses a full connectivity network, and all objects are connected by interfaces to the full connectivity network.

Application of the proposed network construction structure allows to analyse the incoming corporate network and prevent various computer attacks, in particular, various types of DDoS attacks, traffic interception attacks, attacks on web-applications, for example, SQL- and XSS-injections.

The second layer of a fully connected network, which is aimed at analysing internal flows in the corporate network, where cases of infection of company users' workplaces and other devices of the corporate network by virus programs are minimized.

The aim of this work is to implement a two-layer network structure based on full connectivity principles.

The objectives are to develop a model of functioning of the first and second layers of a fully connected network, as well as a model of route formation in the proposed structure and defence against internal and external attacks.

The article uses graph theory and methods, as well as the method of group accounting of arguments.

Keywords: information flow, corporate network, intelligent transport systems, trusted route, trusted process, traffic analyser, fully connected network.

Введение

Вопросы защиты информации остаются приоритетными для всех сфер деятельности. Государственные органы и коммерческие предприятия подвергаются информационным атакам (к ним относятся и информационные объекты ОАО РЖД) обуславливаемыми различными причинами, среди которых выделяются отсутствие импортозамещающих технических средств для реализации сетевого сегмента, проблемы с фильтрацией трафика с целью предотвращения

фишинговых атак, недостаточной развитостью сетевой инфраструктуры, заключающейся в том, что существующие подходы ее реализации не позволяют подходить к этому процессу дифференцировано, то есть создавать условия для защиты информации ориентированные на изменяющиеся и совершенствующие внешние и внутренние атаки, что позволило бы системам защиты информации значительно расширить их функциональные возможности.

В соответствии с Приказом ФСТЭК России «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря 2017 г. № 239 на объектах критической информационной инфраструктуры (объекты информационной инфраструктуры ОАО РЖД относятся именно к таковым) должны быть реализованы различные организационные и технические меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры в соответствии с установленной категорией значимости. Технологии должны реализовать ряд мер, включая следующие: идентификация и аутентификация пользователей и инициируемых ими процессов, разделение полномочий (ролей) пользователей, мониторинг безопасности, контроль целостности программного обеспечения, обеспечение доверенных каналов и маршрутов, с разборкой ранее использованных, реализация систем защиты с использованием одной из моделей дискреционной, мандатной или ролевой, защита от скрытых каналов передачи информации.

Важно отметить, что появление новых IT разработок не только порождает новые способы атак, но и расширяет существующий перечень угроз, а, как известно, каждая угроза может быть осуществлена большим количеством различных атак [1]. Появление новых технологий снижает уровень защищенности существующих систем. В связи с этим на первый план выходит необходимость формирования полного перечня угроз информации, однако данная проблема не имеет простого решения. Для решения этой задачи создаются различные модели угроз, в основе которых лежат всевозможные математические аппараты и информационные модели.

При этом множественность различных моделей обуславливается не только различием взглядов исследователей и их подходов к решению проблемы. Используемые решения задач защиты информации зависят от аспекта информационной безопасности [2]. Мы не можем использовать одни и те же модели для обеспечения защиты конфиденциальности и целостности или доступности, так же как мы не можем использовать одинаковые модели для предсказания атак на информацию и на систему ввиду того, что объекты принципиально отличаются друг от друга. Всем вышесказанным определяется актуальность исследования. Встраивание систем защиты в существующую сетевую структуру требует ее изменения, что неизбежно повышает стоимость любого решения.

Существенно отметить, что вектор направления развития информационных технологий в ОАО РЖД ориентирован на все большее использование интеллектуального подхода в решении задач, стоящих перед транспортной отраслью. В этой связи разработки использующие интеллектуальные методы управления внедряются в повседневную деятельность, а именно [3], [4], [5], [7]:

— цифровой помощник маневрового диспетчера;

— интеллектуальная система Cognitive Rail Pilot;

— программный комплекс Эльбрус-М;

— системы беспилотного движения;

— системы с применением технологии технического зрения на маневровых локомотивах;

— системы прогнозирования размеров грузового движения и пассажирских перевозок.

В статье рассматривается метод построения локальной инфраструктуры с использованием полносвязности. Особенность предлагаемого решения заключается в том, что функционально сеть разделена на два уровня. Первый уровень подключается к сети интернет. На этом уровне расположены защитные ресурсы, а именно различные анализаторы информационных потоков, направленные на анализ поступающего трафика из сети интернет в корпоративную сеть и предотвращающие атаки из внешней сети. Первый уровень представляет собой полносвязную сеть, мощность которой определяется количеством объектов и количеством маршрутов, которые могут быть реализованы в этой сети. В статье рассматриваются простые маршруты, то есть маршруты, не допускающие повторного использования объектов.

Использование методов построения анализаторов с применением искусственных нейронных сетей открывает большие возможности для реализации сложных моделей обработки информационных потоков с целью выявления и предотвращения компьютерных атак на ресурсы компаний. Полносвязность сети открывает возможность параллельной обработки информационных потоков направленных на идентификацию различных типов атак и достаточно эффективное увеличение мощности обработки потоков в случае возрастания потребностей для обработки потоков.

Во втором уровне расположены ресурсы — персональные компьютеры, сервера и другие сетевые объекты. Второй уровень, как и первый, использует полносвязную сеть и все объекты подключаются интерфейсами к полносвязной сети. Но в отличие от первого уровня, на втором проводится анализ внутренних атак, вызванных либо специально направленными действиями злоумышленника, либо ошибочными действиями персонала. В статье рассмотрено построение моделей защиты приложений, функционирующих на первом и втором уровне. Информация из первого уровня передается во второй уровень и наоборот. В статье рассмотрены принципы формирования маршрутов между двумя уровнями.

Отметим следующую особенность, заключающуюся в том, что техническая реализация объектов в полносвязной сети предусматривает использование оптических интерфейсов, работающих на скоростях выше одного гигабита (Gb). Это является преимуществом в реализации предлагаемой структуры сети и открывает широкие перспективы в применении коммутаторов нового поколения со скоростями передачи информации выше одного Gb.

Целью данной работы является реализация двухуровневой структуры сети, построенной на принципах полносвязности.

Задачами являются разработка модели функционирования первого и второго уровней полносвязной сети, а также модели формирования маршрутов в предлагаемой структуре и защита от внутренних и внешних атак.

В статье используются теория и методы графов, а также метод группового учета аргументов.

Решение

Корпоративные сети крупных компаний, в частности ОАО РЖД, в своей деятельности используют подключение к сети интернет, так как большое количество внешних компаний используют ее сервисы для реализации своих бизнес процессов. Это требует реализации строгой политики доступа субъектов и контроля информационных потоков к/из корпоративной сети. Совершенствование технологий нападения со стороны злоумышленников и западных компаний специализирующихся на формировании разнообразных атак требует адекватного ответа, что осуществить, используя существующие методы организации сетей и защиты информации не всегда представляется возможным.

Одним из методов предотвращения атак является метод сборки/разборки маршрута для реализации доступа в сеть субъекта S_i. Это означает, предотвращение повторения маршрута и индентификации субъекта S_i другим субъектом S_{i+1} по параметрам, реализованным для информационного потока от субъекта S_i.

В результате проведенного анализа можно заключить, что в российской законодательной базе нет унифицированного стандарта, содержащего методику формирования политики разграничения доступа. Существующие решения носят частный характер и не учитывают модель информационных потоков в системе, а руководствуются только регламентированным перечнем прав доступа, что не позволяет осуществлять полный контроль над разграничением доступа из-за вероятности появления новых неучтенных ранее информационных потоков. В существующих подходах трудно учесть изменения в модели угроз информации, хотя именно модель угроз позволяет определить возможность появления несанкционированных информационных потоков.

Информационные потоки обозначим is_m – исток и st_m – сток однозначно определяются и не могут быть перепутаны [8], [9], то есть is_m – истоку не может соответствовать st_{m+k} – сток с другим номером. Это определятся требованием корректности субъектов и запускаемыми ими сущностями – приложениями. Приложения, запускаемые на персональных компьютерах или серверах, должны соответствовать требованиям изолированной программной среды [10], [11], [12], а именно:

— корректность: субъекты называются корректными относительно друг друга, когда в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами, ассоциированными с этими субъектами;

— программная среда называется изолированной (ИПС), когда она является замкнутой по порождению субъектов (в ней действует монитор безопасности субъектов (МВС)) и субъекты из порождаемого множества корректны относительного друг друга и монитора безопасности объектов (МВО);

— маршруты в нотации теории графов не ориентированные;

— маршруты простые, то есть в маршруте не может использоваться порт, занятый другим информационным потоком;

— маршруты должны быть реализованы с помощью виртуализации сети и отвечать требованиям $L_f \cap N_f = \varnothing$, где L_f, N_f — разрешенные и неразрешенные маршруты в сети.

В полносвязной сети O_i объект соединяется с O_j объектом через порты, которые обозначим через e, где $i, j = 1, \overline{n}$, где n — количество объектов полносвязной сети. В нотации дискреционной модели имеем:

$$\sum_{k=1}^{N}(O_i \times O_j)_k; N = ((n-1) \times n)/2; i, j = 1, \overline{n}; i \neq j; M = ((n-1) \times n)/2 - 1 \quad (1)$$

где N — количество ребер полносвязной сети или связей между объектами;

M — количество простых маршрутов.

Соединение между объектами полносвязной сети осуществляется через порты. В модели принято следующее, каждый объект нумерует порт по номеру соседнего объекта, с которым он соединяется. Тогда используя (1) для k=1;i=1;j=2 запишем:

$$O_1 e_2 \times e_1 O_2.$$

Каждый объект имеется n-1 связей, которые реализуются через порты. В этой связи представим последнюю формулу (1) следующим образом для произвольных i,j:

$$O_i(\bigcup_{p=1;p\neq i,c_j=1}^{n}(e_p \times c_p)) \times (\bigcup_{p=1;p\neq j,c_i=1}^{n}(e_p \times c_p))O_j \quad (2)$$

де p — номер порта, который не равен номеру своего объекта, а указывает на номер соседнего объекта, к которому он присоединяется;

c_p — переменная указывающая активность порта:

c_p=1, порт активен,

c_p=0, порт закрыт.

Рассмотрим принципы формирования маршрутов в полносвязных сетях в нотации теории графов. Простой маршрут m в полносвязной сети с k_l промежуточными объектами:

$$\begin{gathered} M_m = O_i e_{k_1} \times e_i O_{k_1} e_{k_2} \times e_{k_1} O_{k_2} e_{k_{\dots}} \times \\ \dots \times e_{k_{\dots\dots}} O_{k_l} e_j \times e_{k_l} O_j; i, j, k_1, \dots, k_l = 1, \bar{n} \\ i \neq \langle k_1, \dots, k_l, j \rangle \\ k_1 \neq \langle k_2, \dots, k_l, j \rangle \\ \dots \\ k_l \neq \langle j \rangle, \end{gathered} \quad (3)$$

где k_l — номера промежуточных объектов;

e_{k_l} — порт объекта в полносвязной сети;

$e_i O_{k_1} e_{k_2}$ — соединение объекта O_{k_1} через порты с соседними объектами O_i и O_{k_2} ;

n — количество объектов полносвязной сети.

К ресурсам корпоративной сети ОАО РЖД подключаются пользователи компаний через сеть интернет. Модель доступа легитимного субъекта S_i^l в корпоративную сеть из интернета без технологии полносвязности, с проверкой идентификации (4):

$$((S_i^l) \leftrightarrow H_{ID}^{S_i^l}) \leftrightarrow M_{internet} \leftrightarrow O_{anl} \leftrightarrow O_{Fw} \leftrightarrow (Q_{ID}^{S_i^l} \times O_{srv}^{AD}) \leftrightarrow (O_{srv}^{S_i^l}), \quad (4)$$

где $H_{ID}^{S_i^l}$ — сформированный хеш — идентификационных параметров субъекта S_i^l ;

$M_{internet}$ — маршрут в интернете;

O_{Fw} — объект защитный экран, устанавливает соответствие между протоколом и ip-адресами серверов;

O_{anl} — анализатор информационного потока, может отсутствовать, поскольку проверка легитимности проведена;

O_{srv}^{AD} — сервер AD проверки легитимности пользователя $Q_{ID}^{S_i^l} \times O_{srv}^{AD}$ по $H_{ID}^{S_i^l}$;

$O_{srv}^{S_i^l}$ — сервис, запрашиваемый легитимным пользователем.

Помимо легитимных пользователей возможно подключение внешних пользователей без проверки идентификации S_k^n через сервис почтовых сообщений или web-ресурсы которое описывается следующей структурой:

$$(S_k^n) \leftrightarrow M_{internet} \leftrightarrow O_{anl} \leftrightarrow O_{Fw} \leftrightarrow (O_{srv}^{S_k^n}) \quad (5)$$

где S_k^n — не идентифицированный субъект k;

O_{Fw} — объект защитный экран, устанавливает соответствие между протоколом и ip-адресами серверов;

O_{anl} — анализатор информационного потока.

Как правило, на входе сети дополнительно устанавливается анализатор O_{anl} , выполняющий функции предварительного анализа атак. Необходимо отметить, что различные разработчики предлагают свои решения, содержащие определенный набор фильтрующих функций к анализируемому информационному потоку. Подключение анализаторов, как правило, осуществляется путем их последовательного включения с минимизацией изменений в структуре сети. Ввиду последовательного подключения маршрутизация в сети не изменяется.

Предлагаемая модель реализации сети на основе полносвязности позволяет значительно расширить функциональные возможности для подключения систем защиты — анализаторов. Ввиду значительного изменения сложности атак все большее внимание уделяется применению сложных правил фильтрации с использованием технологии искусственного интеллекта. Изменяется не только сущность атак, но и количественные параметры — ее объемы и продолжительность. Между тем существующие системы имеют существенное временное отставание, при фиксации и уничтожении атаки, так как сбор информации происходит со множества объектов по факту возникновения инцидента. К тому же, сбор информации не автоматизирован.

Формирование маршрутов сервером монитор безопасности объектов (МВО) осуществляется методом группового учета аргументов [13], [14], [15] с выделением маршрутов по критерию на первом ряду (кратчайшие маршруты), на втором ряду (через один промежуточный объект) и так далее. Кратчайший маршрут для передачи информационных потоков с наибольшим приоритетом. Маршруты с промежуточными объектами для информационных потоков с меньшим приоритетом.

Рассмотрим схему, приведенную на рисунке 1. Две полносвязные сети поддерживают формирование маршрутов при помощи сервера $МВО_1$ и $МВО_2$. Между полносвязными сетями установлены связи через объекты. Исходя из формулы (1) опишем маршрут, проходящий от истока is_m находящемуся в полносвязной сети ПС1 к стоку st_m в полносвязной сети ПС2, имеем:

$$M_m = \left(O_i e_{k_1} \times e_i O_{k_1} e_{k_2} \times e_{k_1} O_{k_2} e_{k_{l-s}}\right)_{MBO1} \times \left(e_{k_2} O_{k_{l-s}} e_{k_l} \times e_{k_{l-s}} O_{k_l} e_j \times e_{k_l} O_j\right)_{MBO2};$$

$$\begin{array}{ll} i, k_1, \ldots, k_l = 1, n_1; & k_{l-s}, \ldots, k_l, j = 1, n_2; \\ i \neq \langle k_1, \ldots, k_l \rangle; & k_{l-s} \neq \langle k_{l-1}, k_l, j \rangle; \\ k_1 \neq \langle k_2, \ldots, k_l \rangle; & k_{l-1} \neq \langle k_l, j \rangle; \\ \ldots & \ldots \\ k_{l-1} \neq \langle k_l \rangle; & k_l \neq \langle j \rangle, \end{array} \quad (6)$$

где индексы $МВО_1$ и $МВО_2$ в (6) указывают, что формируются маршруты в ПС1 и ПС2 так, что они должны проходить через объекты (эти объекты назначаются заранее) связывающие эти полносвязные сети, а именно O_{k_2} и $O_{k_{l-s}}$;

n_1, n_2 – количество объектов в полносвязных сетях ПС1 и ПС2.

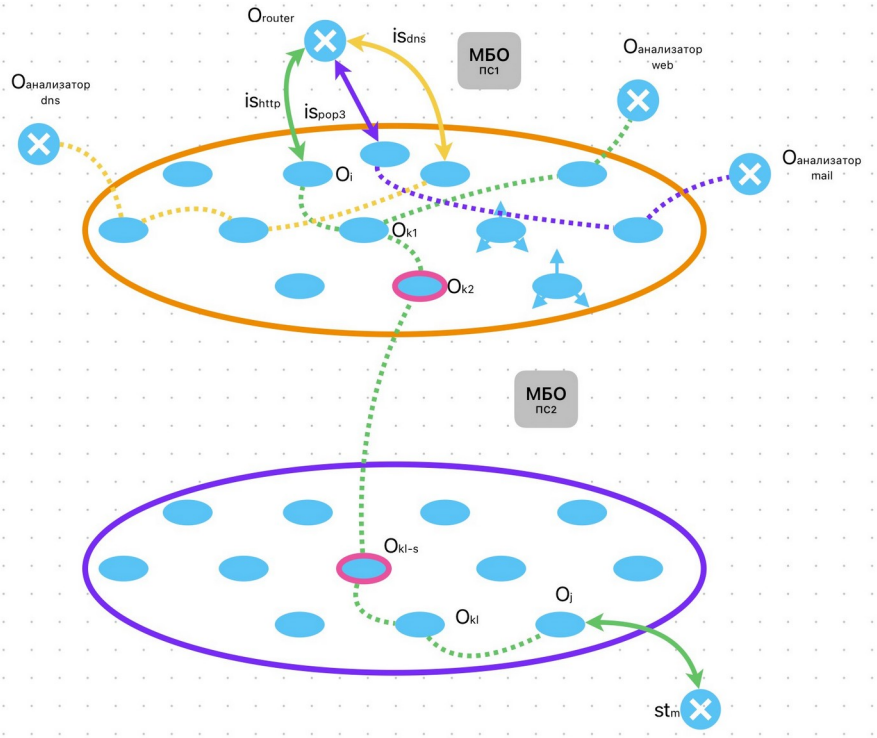

Рисунок 1 - Связь между полносвязными сетями

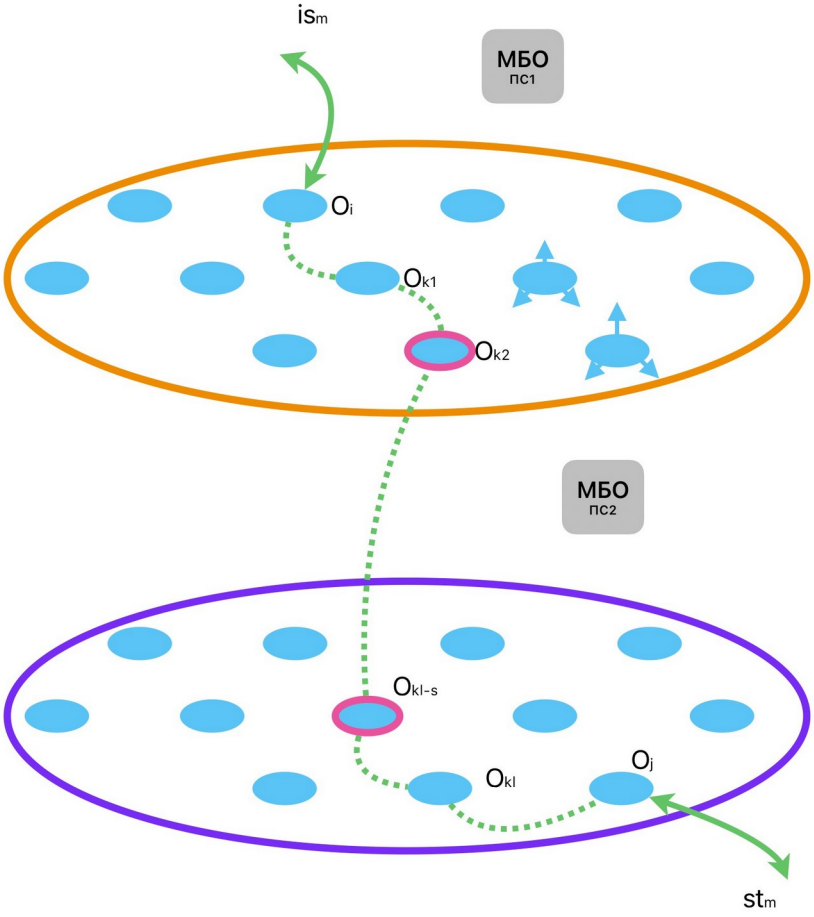

Рисунок 2 - Структура сети с подключенными анализаторами

На рисунке 1 отображен маршрут сформированный в ПС1 и проходящий из этой сети в ПС2 через объекты O_{k_2} и $O_{k_{l-s}}$.

Предложенная структура сети позволяет включить в ПС1 необходимое количество анализаторов информационных потоков с целью анализа и предотвращения атак. Реализация предложенной структуры позволяет включать анализаторы различного типа, что невозможно осуществить при использовании структуры описанной выше.

На рисунке 2 представлена структура ПС1 с включенными анализаторами. Маршрутизатор с интерфейсами e_1, e_2, e_3 подключается к ПС1 по интерфейсам Ethernet с объектами полносвязной сети,

$$O_r e_i, e_{i_1}, e_{i_2} \times (e_1 O_i + e_2 O_{i_1} + e_3 O_{i_2}) \quad (7)$$

где i, i_1, i_2 — номера объектов подключения интерфейсов маршрутизатора O_r с объектами полносвязной сети O_i, O_{i_1}, O_{i_2}.

В рассматриваемой структуре интерфейсы маршрутизатора сконфигурированы на обработку различных протоколов информационных потоков, которые направляются по заданным маршрутам на соответствующие анализаторы. Назначение анализаторов — обнаружение возможной атаки и ее уничтожение. Для реализации этой функции каждый интерфейс e_1,e_2,e_3 маршрутизатора O_r (протокол приписан интерфейсу) соединен через заранее заданный маршрут (нулевой маршрут) M_0 с анализатором на объекте $O_{anl}^{a_t \leftrightarrow pr}$ (настроенном на выявление возможной атаки a_t с использованием этого протокола pr_t $a_t \leftrightarrow pr_t$). Причем заметим, что количество j анализаторов $\bigcup_j (O_{anl}^{a_t \leftrightarrow pr_t})_j; j = 0, \overline{j}$ применяемых к слежение за типом атаки a_t может быть увеличено, с установлением дополнительного маршрута M_j через полносвязную сеть. Увеличение мощности обработки информационного потока обусловлено интенсивностью атаки. Количество анализаторов $\bigcup_j (O_{anl}^{a_t \leftrightarrow pr_t})_j$ устанавливаемых дополнительно определяется заранее, а дополнительные маршруты в зависимости от количества подключенных анализаторов. Причем маршруты M_j заранее не приписываются каждому анализаторов $\bigcup_j (O_{anl}^{a_t \leftrightarrow pr_t})_j$. Это обусловлено тем, что другие типы a_t атак могут использовать свободные объекты и порты полносвязной сети. Отсюда следует, что маршруты M_j формируются в соотвествии с требованием простых маршрутов: не может быть использован один и тоже порт в двух маршрутах одновременно. За увеличивающимся информационным потоком следит специальный анализатор, который дает оповещение на необходимость увеличения мощности обработки потоков в заданном типе атаки a_t. Реализация структуры, приведенной на рисунке 2 для трех интерфейсов маршрутизатора O_r описывается следующей логической зависимостью (8):

$$\begin{aligned} O_r e_i, e_{i_1}, e_{i_2} \times \Bigg(& e_1 O_i e_k \leftrightarrow M_k \leftrightarrow \bigcup_j \left(e_k O_{anl}^{a_{t_1} \leftrightarrow prr_{t_1}} e_{k_c pc_1} \cdots \right)_j + \\ & + e_2 O_{i_1} e_{k_1} \leftrightarrow M_{k1} \leftrightarrow U_j \left(e_{k_1} O_{anl}^{a_{t_2} \leftrightarrow pt_{t_2}} e_{k_c pc_1} \ldots \right)_j + \\ & + e_3 O_{i_2} e_{k_2} \leftrightarrow M_{k2} \leftrightarrow \bigcup_j \left(e_{k_2} O_{anl}^{a_{t_3} \leftrightarrow pr_{t_3}} e_{k_c pc_1} \ldots \right)_j \Bigg), \end{aligned} \quad (8)$$

где $a_{t_1} \leftrightarrow pr_{t_1}$, $a_{t_2} \leftrightarrow pr_{t_2}$, $a_{t_3} \leftrightarrow pr_{t_3}$ — анализаторы атак, использующие протоколы пропускаемые на интерфейсах маршрутизатора O_r;

M_k, M_{k_1}, M_{k_2} — маршруты от интерфейсов маршрутизатора до анализаторов, при выполнении условия простоты маршрутов: $\cup k \neq [\cup k_1, \cup k_2]; \cup k_1 \neq \cup k_2; k, k_1, k_2 = 1, \overline{n}$.

Существенное отличие анализаторов состоит в том, что они не просто фильтруют трафик, а осуществляют более сложную интеллектуальную фильтрацию на основе искусственных нейронных сетей, в заданном признаковом пространстве. Модель анализатора может быть реализована по нескольким моделям искусственных нейронных сетей, в частности сеть Кохонена [16] или перцептрон [17], [18]. Структурно модели очень близки, но главное отличие состоит с том, что расчет сети Кохонена осуществляется итерационной процедурой с использованием метода обратного распространения ошибки, а в случае использования перцептрона расчет осуществляется методом группового учета аргументов [19], [20]. Реализация анализаторов на основе искусственных нейронных сетей не рассматривается в данной статье.

Рассмотрим полносвязную сеть ПС2 изображенную на рисунке 3. Обратимся ко второму уровню. На втором уровне расположены персональные компьютеры пользователей и сервера с приложениями. На втором уровне задаются маршруты от внутренних и внешних пользователей до приложений, размещенных на серверах. Причем для внешних пользователей маршруты проходят из первого уровня после фильтрации анализаторами, а внутренние пользователи маршрутизируются при обращении к ресурсам корпоративной сети с применением аналогичных принципов, как и первом уровне. Как было показано выше связь между полносвязными сетями осуществляется по заранее заданным объектам в соответствии с формулой (3). Количество связей N_c определяет маршруты обмена информацией между полносвязными сетями $M_k^c; k = 1, \overline{N_c}$, где $N_c = n_c^2$, n_c — количество объектов связи [21], [22]. Из первого уровня во второй передаются потоки, формируемые легальными и не идентифицированными пользователями. Анализаторы фильтруют информационные потоки и передают во второй уровень на приложения. Маршруты $M_k^c = \bigcup_{k_c=1}^{n_c} (e_j^{pr_t} O_{k_c}^{pc_1} e_{k_c pc_2} \times e_{k_c pc_1} O_{k_c}^{pc_2} e)$

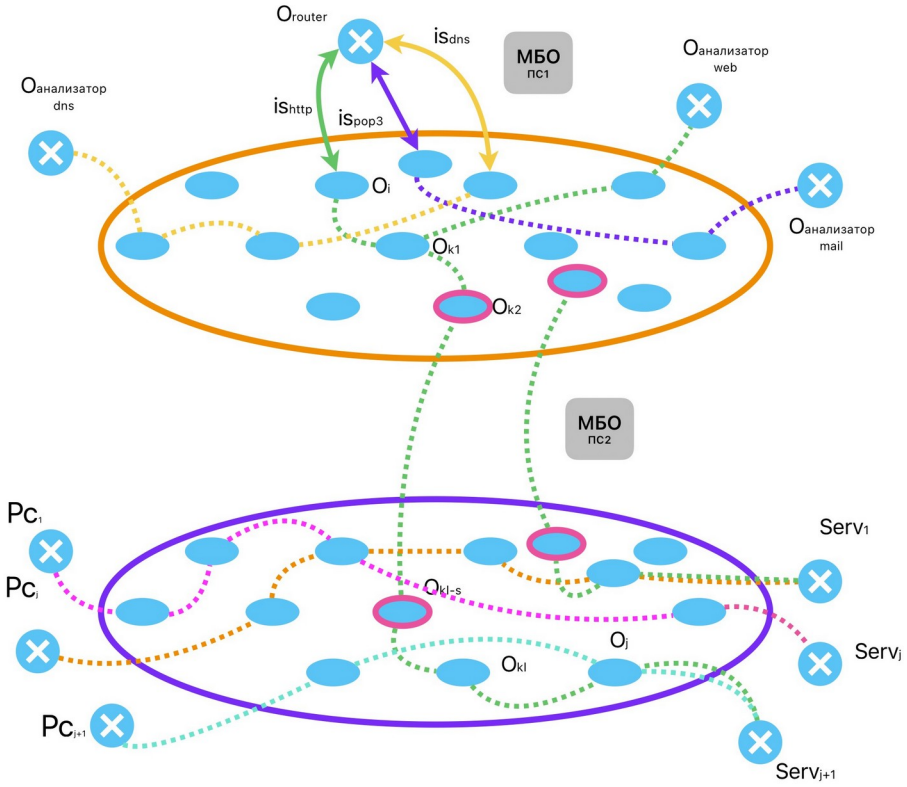

Рисунок 3 - Взаимодействие полносвязных сетей ПС1 и ПС2

Описание маршрутов от маршрутизатора O_r из первого уровня во второй к серверам $O_{srv}^{pr_{t_1}}$, $O_{srv}^{pr_{t_2}}$, $O_{srv}^{pr_{t_2}}$ приведено ниже [22], [23]:

$$O_r e_i, e_{i_1}, e_{i_2} \times \left[\left(e_1 O_i e_k \leftrightarrow M_k^{prr_{t_1}} \leftrightarrow \underset{j}{U_k} \left(e_k O_{anl}^{a_{t_1} \leftrightarrow pr_{t_1}} \right)_j \right)_{MBO_1} \leftrightarrow M_k^c \leftrightarrow \left(M_k^{pr_{t_1}} \leftrightarrow e_k O_{srv}^{pr_{t_1}} \right)_{MBO_2} \right] +$$

$$O_r e_i, e_{i_1}, e_{i_2} \times \left[\left(e_2 O_{i_1} e_{k_1} \leftrightarrow M_k^{prt_{t_2}} \leftrightarrow \bigcup_j \left(e_k O_{anl}^{a_{t_1} \leftrightarrow pr_{t_2}} \right)_j \right)_{MBO_1} \leftrightarrow M_k^c \leftrightarrow \left(M_k^{prt_2} \leftrightarrow e_k O_{srv}^{prt_2} \right)_{MBO_2} \right] +$$

$$O_r e_i, e_{i_1}, e_{i_2} \times \left[\left(e_3 O_{i_2} e_{k_2} \leftrightarrow M_k^{pr_{t_3}} \leftrightarrow \bigcup_j \left(e_{k_2} O_{anl}^{at_{t_3} \leftrightarrow pr_{t_3}} \right)_j \right)_{MBO_1} \leftrightarrow M_k^c \leftrightarrow \left(M_k^{pr_{t_3}} \leftrightarrow e_k O_{srv}^{pr_{t_3}} \right)_{MBO_2} \right],$$

Во втором уровне субъекты (персонал) S_i^l через персональные компьютеры O^рсобращаются к ресурсам корпоративной сети. Запуском информационного потока является инициализация приложения pl_j легальным субъектом S_i^l на персональном компьютере $O_{pl_j}^{pc}$, которое связывается с сервером $O_{srv}^{pr_t}$, где pr_t — протокол обмена приложения и сервера. В корпоративной сети могут одновременно существовать большое количество информационных потоков, обусловленных потребностями персонала и различных интеллектуальных технологических систем.

Сервер $МВО_2$ контролирует работу субъектов S_i^l на персональных компьютерах, имеющих различные уровни доступа D_i. Инициализация приложения pl_j на персональном компьютере отмечается в $МВО_2$ номером информационного потока j, которому будет соответствовать is_j — исток (от объекта O^{pc_i}) и st_j — сток (сервер $O_{srv}^{pr_t}$), проходящие по маршруту M_j, который заранее сгенерирован в сервере $МВО_2$. Схема взаимодействия описывается $((S_i^l \times D_i) \times O_{pl_j}^{pc_i})_{is_j} \leftrightarrow M_j \leftrightarrow (O_{srv}^{pr_t})_{st_j}$. Описание взаимодействия в нотации дискреционной модели [22], [24], [25]:

$$((S_i^l \times D_i) \times O_{pl_j}^{pc_i} e_j)_{is_j} \leftrightarrow M_j \leftrightarrow (H_{ID}^{S_i^l} \times e_j O_{srv}^{pr_t})_{st_j}, \quad (9)$$

где $(S_i^l \times D_i)$ — дискреционный доступ субъекта S_i^l к объекту $O_{pl_j}^{pc_i}$ с интерфейсом e_j;

M_j — маршрут в полносвязной сети ПС2 (9) определяемый формулой (1);

$(H_{ID}^{S_i^l} \times e_j O_{srv}^{pr_t})$ - идентификация субъекта S_i^l на сервере $O_{srv}^{pr_t}$ с интерфейсом e_j соответствующим маршруту M_j;

$H_{ID}^{S_i^l}$ — хеш - функция проверки легальности субъекта S_i^l;

is_j, st_j — исток и сток маршрута M_j.

Персональные компьютеры O^{pc_i} подключены к полносвязной сети ПС2. Сервера с приложениями также подключаются к сети ПС2 (рисунок 3). Маршруты от персональных компьютеров строятся аналогично рассмотренной выше модели. Особенность построения маршрутов заключается в том, что по разным маршрутам возможно обращаться к одному и тому же серверу. Но, так как это разные виртуальные сети, на сервере выстраивается очередь из запросов из нескольких виртуальных маршрутов M_k и сервер формирует ответ каждому запросу.

Техническая реализация управления в двухуровневой полносвязной сети

Управление полносвязными сетями требует сложных систем мониторинга и управления для обеспечения бесперебойной работы и оптимизации трафика. Используются различные протоколы и системы управления [26], [27]:

— SNMP (Simple Network Management Protocol) реализует мониторинг состояния сети и управления ею.

— SDN (Software-Defined Networking) позволяет гибко управлять сетевой инфраструктурой и адаптировать маршрутизацию в реальном времени.

В работе за основу принята SDN. В SDN управление сетью отделяется от физического оборудования и реализуется на уровне программного обеспечения. Это обеспечивает большую гибкость и контроль над сетевой инфраструктурой. Контроллер SDN централизованно управляет всей сетевой инфраструктурой. Важными характеристиками являются программируемость: SDN позволяет программировать поведение сети, используя открытые интерфейсы и протоколы, такие как OpenFlow и виртуализация: сети могут быть виртуализированы для создания различных виртуальных сетей (VLANs, VPNs и т.д.) на одном физическом оборудовании, что позволяет эффективнее использовать ресурсы.

Реализация SDN осуществлена с применением Ryu — который предоставляет возможности для управления сетями и разработанными сетевыми приложениями, написан на языке программирования Python. Ryu управляет сетевыми устройствами через каналы-порты:

— OpenFlow порт — порт 1 слушает OpenFlow-соединения от коммутаторов и управляет установкой и обновлением правил потоков. Коммутаторы (или другие сетевые устройства) и контроллер используют IP-адреса для установления и поддержания TCP-соединений. Контроллер слушает на определённом IP-адресе и порту (например, 6653 по умолчанию), а сетевые устройства инициируют соединение с контроллером через этот адрес и порт.

— REST API порт — порт 2 предоставляет интерфейс для внешних систем и приложений, позволяя взаимодействовать с контроллером через HTTP/HTTPS запросы. REST API предоставляет интерфейс для внешних приложений и служб, которые взаимодействуют с контроллером через HTTP/HTTPS. Эти запросы направляются на IP-адрес и порт, где REST API контроллера доступен (порт 8080 по умолчанию).

— NETCONF порт — порт 3 используется для управления конфигурацией сетевых устройств с помощью NETCONF. NETCONF, используемый для управления конфигурацией сетевых устройств, также работает через IP. Устройства и контроллер взаимодействуют по IP-адресам, используя TCP для передачи данных. Стандартный порт для NETCONF — 830.

Клиентская библиотека — ncclient позволяет контроллеру RYU взаимодействовать с сетевыми устройствами по протоколу NETCONF.

На рисунке 4 показана реализация тестовой двухуровневой полносвязной сети. Сервера формирования маршрутов в полносвязных сетях На маршрутизаторе O_r связи с интернетом установлены четыре порта e_0, e_1, e_2, e_3. Порт e_1 — сконфигурирован под пропуск протокола HTTPs/HTTP и направляется по маршруту до анализатора ddos — атаки. Порт e_2 — сконфигурирован для пропуска протокола POP3 направляемый к mail — анализатору

Порт e_3 — сконфигурирован для пропуска пакетов протокола TCP/IP и направлен к анализатору приложений. Анализаторы проверяют в заданном признаковом пространстве наличие аномалии в пакетах информационных потоков и отправляют их по маршруту между полносвязными сетями до серверов, в случае ее отсутствия.

Из базы данных Digital Attack Map [28] посылаются пакеты с атаками ddos направленными на сервер web, фишинг-атаки [29], [30] направлены на почтовый сервер mail, а атаки, связанные с проникновением вирусов [31] направлены на приложение – формирование расписания движения на участке железной дороги. Корпоративная сеть на втором уровне ПС2 через маршрутизатор PE связана с клиентским маршрутизатором CE, которым управляет Ryu посредством протокола NETCONF. Сервер MBO_1 формирует маршруты от O_r до анализаторов посредством конфигурирования VLAN IDe_i. IDe_i — номер виртуальной сети по маршруту от портов e_1, e_2, e_3 маршрутизатора O_r до анализаторов через промежуточные объекты коммутаторы. По всему маршруту осуществляется конфигурация объектов, через которые проходит маршрут, прописываются VLAN IDe_i на портах промежуточных объектов (коммутаторах) и портах анализатора. Это осуществляет Ryu на основании сформированного маршрута сервером MBO_1, который отправляет данные о маршруте по интерфейсу REST API. Внутри одной VLAN для передачи данных между устройствами IP-адресация не требуется, так как кадры направляются на основе MAC-адресов и VLAN IDe_i. Анализаторы имеют два интерфейса, по которым принимаются пакеты информационного потока и отправляются во вторую полносвязную сеть через объекты связи по маршрутам между корпоративными сетями. На рисунке 4 показан маршрут от порта маршрутизатора e_1 до анализатора ddos-атак от маршрутизатора по виртуальной сети обозначенный на рисунке 4, как VLAN IDe_1. Далее через второй порт анализатор ddos-атак отправляет пакеты через объекты связи между полносвязными сетями по одному из маршрутов. Далее маршрут прокладывается сервером MBO_2 до сервера web. Признаком для формирования маршрута являются протокол и порт e_1 маршрутизатора O_r.

В отличие от приведенной тестовой структуры порты маршрутизатора могут быть сконфигурированы для пропуска различных протоколов. Маршруты определяются в зависимости от пропускаемого протокола.

Информация об информационном потоке, содержащем пакеты определенного типа, передается на Ryu по OpenFlow – сообщения статистики и состояния Stats Request/Reply – используются для запроса статистических данных, таких как статистика портов, потоков, групп и таблиц потоков. Эти данные позволяют отслеживать текущую ситуацию формированию маршрутов.

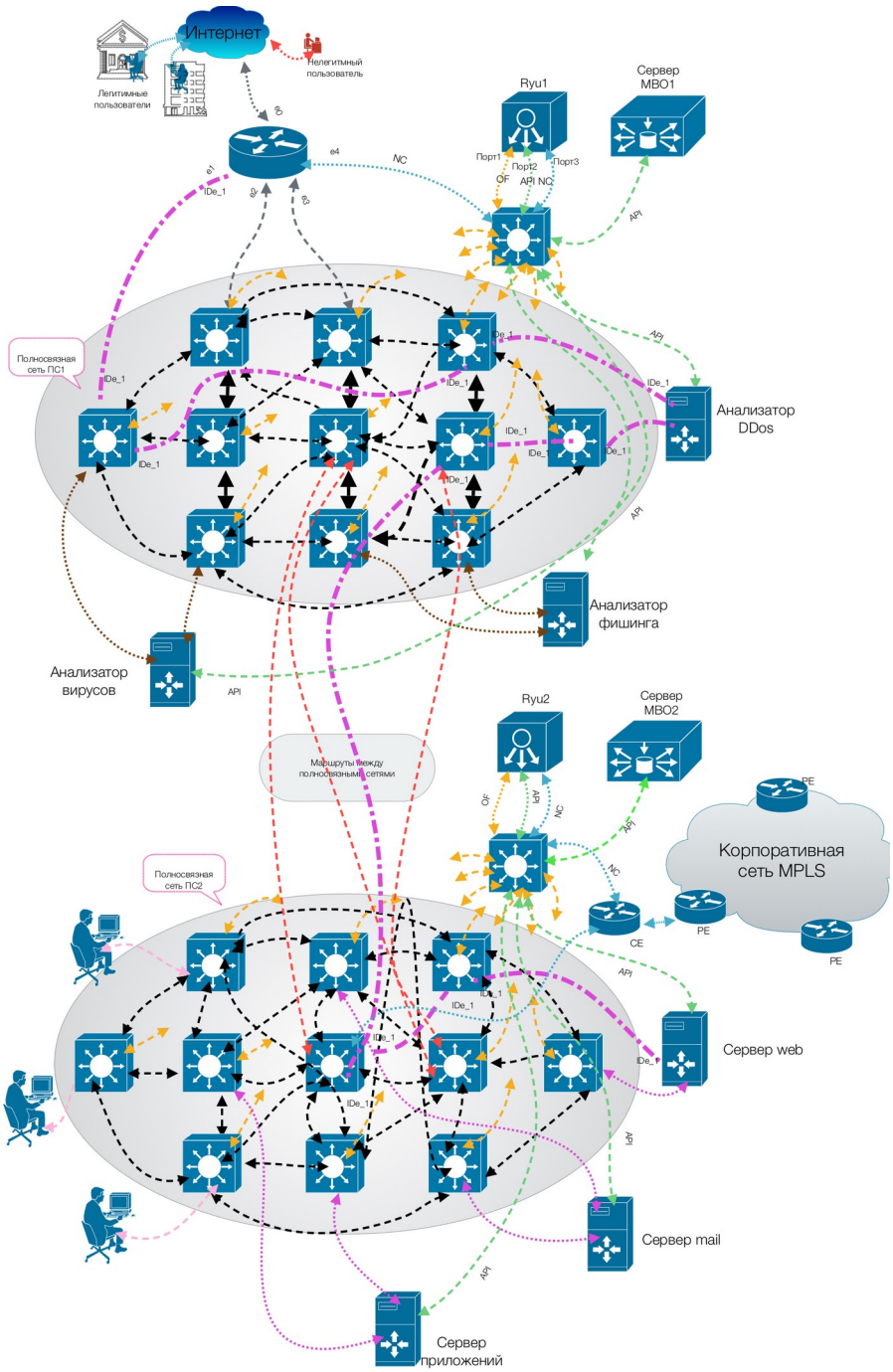

Рисунок 4 - Структура двухуровневой полносвязной сети

Обсуждение

Применение предложенной структуры построения сети позволяет анализировать входящий в корпоративную сеть и предотвращать различные компьютерные атаки. В частности, различные виды DDoS атак, атаки перехвата трафика, атаки на web-приложения, например, SQL- и XSS-инъекции.

Благодаря второму уровню полносвязной сети, который направлен на анализ внутренних потоков в корпоративной сети, минимизируются случаи заражения рабочих мест пользователей компании и других устройств корпоративной сети вирусными программами. Сводится к минимуму эффективность фишинговых рассылок, поскольку даже при запуске вредоносного вложения или переходу по ссылке на вредоносный ресурс данная активность со стороны внутреннего субъекта моментально блокируется.

Принимая во внимание постоянно растущую активность хакерских группировок в отношении государственных и коммерческих организаций Российской Федерации, предотвращение вышеуказанных атак используя новые технологии является актуальным вопросом на текущий момент.

Особое значение предлагаемая технология имеет для обеспечения защиты информации в интеллектуальных транспортных системах, относящихся к критической информационной инфраструктуре, требования к безопасности которых регламентируются Федеральными законами, Постановлениями Правительства Российской Федерации, приказами Президента РФ и приказами и нормативными актами регуляторов в сфере информационной безопасности.

Проведенный анализ по материалам научных публикаций [32], [34], [36], [39] показывает, что применение технологии многоуровневой защиты является актуальным направлением. Новизна предлагаемого решения характеризуется несколькими пунктами:

— анализаторы (выполняющие функции распознавания атак) должны устанавливаться на различных уровнях системы защиты;

— маршрутизация между уровнями осуществляется по маршрутам задаваемым сервером безопасности объектов (выбор маршрута случаен), при полной проверке субъекта запрашивающего соединение;

— на каждом уровне соединение объектов должно осуществляться с использованием полносвязной сети с предоставлением маршрута легитимному пользователю и отказом нелегитимному пользователю или вредоносному приложению.

Предложенное решение предотвращает возможность проникновения нелегитимному субъекту или вредоносному ПО между уровнями.

Заключение

В статье рассмотрены принципы построения двухуровневой структуры построения сети на основе использования принципа полносвязности. Решены задачи формирования маршрутов на первом и втором уровнях, а также связи между уровнями. На первом уровне соединенном с интернетом решаются задачи анализа поступающего трафика может быть использовано для предотвращения атак большое количество интеллектуальных анализаторов позволяющих повысить качество анализа. При этом полносвязная сеть позволяет организовывать одновременно множество маршрутов, что позволяет прейти к параллельной обработке входящего трафика.

Второй уровень структуры ориентирован на формирование маршрутов пользователям корпоративной сети с серверным оборудованием, а также легальным пользователям из сети интернет. На втором уровне осуществляется защита от внутренних атак. Осуществлена техническая реализация двухуровневой системы защиты информации.

Новизна предлагаемого решения характеризуется несколькими пунктами:

— анализаторы (выполняющие функции распознавания атак) должны устанавливаться на различных уровнях системы защиты;

— маршрутизация между уровнями осуществляется по маршрутам задаваемым сервером безопасности объектов (выбор маршрута случаен), при полной проверке субъекта, запрашивающего соединение;

— на каждом уровне соединение объектов должно осуществляться с использованием полносвязной сети с предоставлением маршрута легитимному пользователю и отказом нелегитимному пользователю или вредоносному приложению.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Егошин Н.С. Модель угроз безопасности информации, передаваемой через интернет / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Информация и безопасность. — 2018. — Т. 21. — № 4. — С. 530–533.
2. Егошин Н.С. Формирование модели нарушителя / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Безопасность информационных технологий. — 2017. — Т. 24. — № 4. — С. 19–26. — DOI: 10.26583/bit.2017.4.02.
3. Карпов О. Евгений Чаркин, заместитель генерального директора РЖД: «Искусственный интеллект будет интегрирован в большинство сервисов РЖД в ближайшие 10-15 лет» / О. Карпов // Комсомольская правда. — 2023. — 26 декабря. — URL: https://www.kp.ru/daily/27599/4871733/ (дата обращения: 19.04.2024).
4. Якимова С. Искусственный интеллект организует движение на железной дороге / С. Якимова. — URL: https://rzddigital.ru/projects/iskusstvennyy-intellekt-organizuet-dvizhenie-na-zheleznoy-doroge-/ (дата обращения: 19.04.2024).
5. Зубов А. Нейросеть сортирует вагоны / А. Зубов // Газета Гудок. — 2020. —24 сентября (№ 178 (27027)).
6. Филиппова А. Железная дорога попалась в нейросеть / А. Филиппова. — URL: https://company.rzd.ru/ru/9401/page/78314?id=210366&ysclid=lt1okbmzz2510294992 (дата обращения: 19.04.2024).
7. Крупин А. РЖД доверила управление расписанием поездов искусственному интеллекту / А. Крупин. — URL: https://3dnews.ru/1080514/rgd-doverila-upravlenie-marshrutami-poezdov-iskusstvennomu-intellektu (дата обращения: 19.04.2024).
8. Кормен Т.Х. Алгоритмы: построение и анализ / Т.Х. Кормен, Ч.И. Лейзерсон, Р.Л. Ривест [и др.]. — М.: Вильямс, 2009. — 1290 с.
9. Bandelt H.-J. Combinatorics and geometry of finite and infinite squaregraphs / H.-J. Bandelt, V. Chepoi, D. Eppstein // SIAM Journal on Discrete Mathematics. — 2010. — Vol. 24. — Iss. 4. — P. 1399–1440. — DOI: 10.1137/090760301.
10. Девянин П.Н. Модели безопасности компьютерных систем / П.Н. Девянин. — Москва: Горячая Линия-Телеком, 2023. — 353 с.
11. Браницкий А.А. Построение нейросетевой и иммуноклеточной системы обнаружения вторжений / А.А. Браницкий, И.В. Котенко // Проблемы информационной безопасности. Компьютерные системы. — 2015. — № 4. — С. 23–27.
12. Штеренберг С.И. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой / А.В. Красов, М.В. Левин, С.И.,Штеренберг [и др.] // Наукоемкие технологии в космических исследованиях Земли. — 2016. — Т. 8. — № 4. — С. 70–74.

13. Ивахненко А.Г. Индуктивный метод самоорганизации моделей сложных систем / А.Г. Ивахненко. — Киев: Наукова думка, 1981. — 325 с.
14. Ивахненко А.Г. Помехоустойчивость моделирования / А.Г. Ивахненко, В.С. Степашко. — Киев: Наукова думка, 1985. — 197 с.
15. Стрижов В.В. Методы выбора регрессионных моделей / В.В. Стрижов, Е.А. Крымова. — М.: ВЦ РАН, 2010. — 55 с.
16. Солдатова О.П. Исследование эффективности решения задачи классификации гибридными сетями кохонена / О.П. Солдатова, П.Д. Чайка // Известия Самарского научного центра Российской академии наук. — 2015. — Т. 17. — № 2 (5). — С. 1147–1152.
17. Розенблатт Ф. Принципы нейродинамики: Перцептроны и теория механизмов мозга / Ф. Розенблатт. — М.: Мир, 1965. — 480 с.
18. Хайкин С. Нейронные сети: Полный курс / С. Хайкин. — М.: Вильямс, 2006. — 1104 с.
19. RoboCraft. — URL: https://robocraft.ru/algorithm/560 (дата обращения: 22.06.2024).
20. Зуев В.Н. Модифицированный алгоритм обучения нейронных сетей / В.Н. Зуев, В.К. Кемайкин // Программные продукты и системы. — 2019. — № 2 (32). — С. 258–262. — DOI: 10.15827/0236-235X.126.258-262.
21. Волков Е.А. Численные методы / Е.А. Волков. — М.: Физматлит, 2003.
22. Алексеев В.М. Защита информации в интеллектуальных транспортных системах управления городским транспортом / В.М. Алексеев, С.Н. Чичков // Надежность. — 2022. — № 22 (3). — С. 62–68. — DOI: 10.21683/1729-26462022-22-3-62-68.
23. Смышляев С.В. Математические методы обоснования оценок уровня информационной безопасности программных средств защиты информации, функционирующих в слабодоверенном окружении: автореф. дис. ... д-ра тех. наук / Смышляев Станислав Витальевич. — 2021.
24. Кирилов А.С. Метод обнаружения и кластеризации вредоносного программного обеспечения с использованием признаков декларируемого и фактического функционала: автореф. дис. ... канд. техн. наук / Кириллов Алексей Сергеевич. — 2022.
25. Embersim: большая база данных для ускоренного поиска сходств в анализе вредоносного ПО. — URL: https://iitd.com.ua/ru/news/embersim-velika-baza-danih-dlya-priskorenogo-poshuku-pod-bnostey-v-anal-z-shk-dlivogo-pz/ (дата обращения: 09.07.2024).
26. Мясников А.В. Построение модели информационной системы для применения в автоматизации тестирования на проникновение / А.В. Мясников // Проблемы информационной безопасности. Компьютерные системы. — СПб., 2020. — № 3. — С. 32–39.
27. Ошкина Е.В. Сетевая технология SDN (обзор, современные тенденции) / Е.В. Ошкина // Технические науки: проблемы и перспективы : материалы V Междунар. науч. конф. (г. Санкт-Петербург, июль 2017 г.). — Санкт-Петербург : Свое издательство, 2017. — С. 3–6. — URL: https://moluch.ru/conf/tech/archive/231/12628/ (дата обращения: 29.07.2024).
28. Digital Attack Map. — URL: https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18763&view=map (accessed: 06.08.2024).
29. Phishstats. — URL: https://phishstats.info (accessed: 06.08.2024).
30. Phishtank. — URL: https://www.phishtank.com (accessed: 06.08.2024).
31. Virustotal. — URL: https://www.virustotal.com/gui/home/url (accessed: 06.08.2024).

Список литературы на английском языке / References in English

1. Egoshin N.S. Model' ugroz bezopasnosti informacii, peredavaemoj cherez internet [Model of threats to the security of information transmitted via the Internet] / N.S. Egoshin, A.A. Konev, A.A. Shelupanov // Informacija i bezopasnost' [Information and Safety]. — 2018. — Vol. 21. — № 4. — P. 530–533. [in Russian]
2. Egoshin N.S. Formirovanie modeli narushitelja [Formation of the intruder model] / N.S. Egoshin, A.A. Konev, A.A. Shelupanov // Bezopasnost' informacionnyh tehnologij [Security of information technologies]. — 2017. — Vol. 24. — № 4. — P. 19–26. — DOI: 10.26583/bit.2017.4.02. [in Russian]
3. Karpov O. Evgenij Charkin, zamestitel' general'nogo direktora RZhD: «Iskusstvennyj intellekt budet integrirovan v bol'shinstvo servisov RZhD v blizhajshie 10-15 let» [Evgeny Charkin, Deputy Director General of Russian Railways: "Artificial Intelligence will be integrated into the majority of RZD services in the next 10-15 years"] / O. Karpov // Komsomolskaya Pravda. — 2023. — 26 December. — URL: https://www.kp.ru/daily/27599/4871733/ (accessed: 19.04.2024). [in Russian]
4. Jakimova S. Iskusstvennyj intellekt organizuet dvizhenie na zheleznoj doroge [Artificial intelligence organizes traffic on railways] / S. Jakimova. — URL: https://rzddigital.ru/projects/iskusstvennyy-intellekt-organizuet-dvizhenie-na-zheleznoy-doroge-/ (accessed: 19.04.2024). [in Russian]
5. Zubov A. Nejroset' sortiruet vagony [A neural network sorts the wagons] / A. Zubov // Gazeta Gudok. — 2020. —24 September (№ 178 (27027)). [in Russian]
6. Filippova A. Zheleznaja doroga popalas' v nejroset' [The railway got caught in a neural net] / A. Filippova. — URL: https://company.rzd.ru/ru/9401/page/78314?id=210366&ysclid=lt1okbmzz2510294992 (accessed: 19.04.2024). [in Russian]
7. Krupin A. RZhD doverila upravlenie raspisaniem poezdov iskusstvennomu intellektu [RZD has entrusted the management of train schedules to artificial intelligence] / A. Krupin. — URL: https://3dnews.ru/1080514/rgd-doverila-upravlenie-marshrutami-poezdov-iskusstvennomu-intellektu (accessed: 19.04.2024). [in Russian]
8. Cormen T.H. Algoritmy: postroenie i analiz [Algorithms: construction and analysis] / T.H. Cormen, C.I. Leiserson, R.L. Rivest [et al.]. — M.: Williams, 2009. — 1290 p. [in Russian]

9. Bandelt H.-J. Combinatorics and geometry of finite and infinite squaregraphs / H.-J. Bandelt, V. Chepoi, D. Eppstein // SIAM Journal on Discrete Mathematics. — 2010. — Vol. 24. — Iss. 4. — P. 1399–1440. — DOI: 10.1137/090760301.

10. Devjanin P.N. Modeli bezopasnosti komp'juternyh sistem [Security models for computer systems] / P.N. Devjanin. — Moscow: Hotline-Telecom, 2023. — 353 p. [in Russian]

11. Branickij A.A. Postroenie nejrosetevoj i immunokletochnoj sistemy obnaruzhenija vtorzhenij [Construction of neural network and immunocellular system of intrusion detection] / A.A. Branickij, I.V. Kotenko // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy [Problems of information security. Computer systems]. — 2015. — № 4. — P. 23–27. [in Russian]

12. Shterenberg S.I. Model' upravlenija potokami trafika v programmno-opredeljaemoj seti s izmenjajushhejsja nagruzkoj [Traffic flow control model in software-defined network with changing load] / A.V. Krasov, M.V. Levin, S.I.,Shterenberg [et al.] // Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli [Science-intensive technologies in Earth's space research]. — 2016. — Vol. 8. — № 4. — P. 70–74. [in Russian]

13. Ivahnenko A.G. Induktivnyj metod samoorganizacii modelej slozhnyh sistem [Inductive method of self-organization of models of complex systems] / A.G. Ivahnenko. — Kyiv: Naukova dumka, 1981. — 325 p. [in Russian]

14. Ivahnenko A.G. Pomehoustojchivost' modelirovanija [Modelling noise immunity] / A.G. Ivahnenko, V.S. Stepashko. — Kyiv: Naukova dumka, 1985. — 197 p. [in Russian]

15. Strizhov V.V. Metody vybora regressionnyh modelej [Methods for selecting regression models] / V.V. Strizhov, E.A. Krymova. — M.: VC RAS, 2010. — 55 p. [in Russian]

16. Soldatova O.P. Issledovanie jeffektivnosti reshenija zadachi klassifikacii gibridnymi setjami kohonena [A study of the efficiency of solving the classification problem by hybrid kohonen networks] / O.P. Soldatova, P.D. Chajka // Izvestija Samarskogo nauchnogo centra Rossijskoj akademii nauk [Proceedings of the Samara Scientific Centre of the Russian Academy of Sciences]. — 2015. — Vol. 17. — № 2 (5). — P. 1147–1152. [in Russian]

17. Rosenblatt F. Principy nejrodinamiki: Perceptrony i teorija mehanizmov mozga [Principles of neurodynamics: Perceptrons and the theory of brain mechanisms] / F. Rosenblatt. — M.: Mir, 1965. — 480 p. [in Russian]

18. Haykin S. Nejronnye seti: Polnyj kurs [Neural Networks: A Complete Course] / S. Haykin. — M.: Williams, 2006. — 1104 p. [in Russian]

19. RoboCraft. — URL: https://robocraft.ru/algorithm/560 (accessed: 22.06.2024). [in Russian]

20. Zuev V.N. Modificirovannyj algoritm obuchenija nejronnyh setej [Modified algorithm of neural networks training] / V.N. Zuev, V.K. Kemajkin // Programmnye produkty i sistemy [Software Products and Systems]. — 2019. — № 2 (32). — P. 258–262. — DOI: 10.15827/0236-235X.126.258-262. [in Russian]

21. Volkov E.A. Chislennye metody [Numerical methods] / E.A. Volkov. — M.: Fizmatlit, 2003. [in Russian]

22. Alekseev V.M. Zashhita informacii v intellektual'nyh transportnyh sistemah upravlenija gorodskim transportom [Information protection in intelligent transport systems of urban transport management] / V.M. Alekseev, S.N. Chichkov // Nadezhnost' [Reliability]. — 2022. — № 22 (3). — P. 62–68. — DOI: 10.21683/1729-26462022-22-3-62-68. [in Russian]

23. Smyshljaev S.V. Matematicheskie metody obosnovanija ocenok urovnja informacionnoj bezopasnosti programmnyh sredstv zashhity informacii, funkcionirujushhih v slabodoverennom okruzhenii [Mathematical methods of substantiation of assessments of the information security level of information protection software operating in a weakly trusted environment]: abst. dis. ... PhD in Technical Sciences / Smyshljaev Stanislav Vital'evich. — 2021. [in Russian]

24. Kirilov A.S. Metod obnaruzhenija i klasterizacii vredonosnogo programmnogo obespechenija s ispol'zovaniem priznakov deklariruemogo i faktycheskogo funkcionala [A method for detecting and clustering malicious software using features of declared and actual functionality]: abst. dis. ... PhD in Technical Sciences / Kirillov Aleksej Sergeevich. — 2022. [in Russian]

25. Embersim: bol'shaja baza dannyh dlja uskorennogo poiska shodstv v analize vredonosnogo PO [Embersim: a large database for accelerated similarity search in malware analysis]. — URL: https://iitd.com.ua/ru/news/embersim-velika-baza-danih-dlya-priskorenogo-poshuku-pod-bnostey-v-anal-z-shk-dlivogo-pz/ (accessed: 09.07.2024). [in Russian]

26. Mjasnikov A.V. Postroenie modeli informacionnoj sistemy dlja primenenija v avtomatizacii testirovanija na proniknovenie [Information system model construction for application in penetration testing automation] / A.V. Mjasnikov // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy [Problems of information security. Computer systems]. — SPb., 2020. — № 3. — P. 32–39. [in Russian]

27. Oshkina E.V. Setevaja tehnologija SDN (obzor, sovremennye tendencii) [SDN network technology (review, current tendencies)] / E.V. Oshkina // Tehnicheskie nauki: problemy i perspektivy : materialy V Mezhdunar. nauch. konf. (g. Sankt-Peterburg, ijul' 2017 g.) [Technical Sciences: problems and prospects : proceedings of the V International Scientific Conference (St. Petersburg, July 2017)]. — St.Petersburg : Svoe Publishing, 2017. — P. 3–6. — URL: https://moluch.ru/conf/tech/archive/231/12628/ (accessed: 29.07.2024). [in Russian]

28. Digital Attack Map. — URL: https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18763&view=map (accessed: 06.08.2024).

29. Phishstats. — URL: https://phishstats.info (accessed: 06.08.2024).

30. Phishtank. — URL: https://www.phishtank.com (accessed: 06.08.2024).

31. Virustotal. — URL: https://www.virustotal.com/gui/home/url (accessed: 06.08.2024).