УДК 519.687

Ушаков Ю.А., Коннов А.Л., Полежаев П.Н., Шухман А.Е.
Оренбургский государственный университет
E-mail: unpk@mail.ru

ИМИТАЦИОННАЯ МОДЕЛЬ САМООРГАНИЗУЮЩЕЙСЯ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

В настоящее время виртуальные частные сети (VPN) широко используются для соединения распределенных сетевых сегментов. Нами разработана концепция самоорганизующейся виртуальной частной сети на основе облачных технологий. Развертывание VPN может быть значительно упрощено с использованием автоматической настройки сетевых устройств на основе различных алгоритмов, определяющих топологию сети, а также методов маршрутизации.

Исследование алгоритмов управления и маршрутизации VPN может быть выполнено на основе имитационного моделирования. В статье представлена имитационная модель самоорганизующейся VPN. В результате тестирования была выявлена зависимость возрастания нагрузки сети в случае отказа связи между узлами. Имитационная модель сети VPN может быть использована для проведения экспериментов на любых топологиях, а также для разработки симулятора сегмента сети.

Ключевые слова: виртуальные частные сети, имитационная модель, программно-конфигурируемые сети, сеть как сервис.

Введение

В современном бизнесе для поддержания информационной инфраструктуры необходимо широкое использование различных коммуникационных сервисов с высоким качеством услуг и приемлемым уровнем информационной безопасности. Готовые решения по развертыванию виртуальных частных сетей очень дороги по стоимости и требуют высокой квалификации администраторов.

Нами разработана концепция самоорганизующейся виртуальной частной сети на основе облачных технологий [1]. Применение такого подхода к предоставлению сетевых услуг позволяет осуществлять доступ и совместное использование сетевых ресурсов по модели доступа NaaS (Network-as-a-Service), не осуществляя их запуск на локальном узле. Нами предлагается использование средств удаленного администрирования для автоматической настройки маршрутизаторов.

Для реализации VPN соединений были выбраны технологии IPSEC/L2TP и OpenVPN в качестве альтернативы в случае плохих каналов, ограничений провайдеров и т. п. Для маршрутизации и изоляции трафика используется связка OpenFlow и OpenVSwitch, VRF и OSPF, для этого требуется реализация алгоритма предварительного расчета топологии, например, на основе генетических или муравьиных алгоритмов обхода дерева [2].

Масштабное исследование поведения различных алгоритмов маршрутизации для разных сетевых топологий целесообразно выполнять с помощью имитационного моделирования.

Имитационная модель работы VPN сети

Разработка имитационной модели работы самоорганизующейся частной виртуальной сети с частичной связностью узлов, многопутевой маршрутизацией, обеспечением QoS является многосоставной задачей. Реализация узла облачного VPN-сервера (рисунок 1) с виртуальными Docker OpenVPN серверами начинается с узла обработки маршрутов, которым является входящий распределитель VPN подключений

Реализация многопутевой маршрутизации основана на облаке, которое состоит из множества маршрутизаторов с частичной связностью и параллельными маршрутами:

На основе этих моделей собирается общая модель сети. Схема построения подобной сети представлена на рисунке 3.

Для реализации имитационной модели данной сети была использована среда моделирования Riverbed Modeler с набором стандартных компонент:

Существует несколько способов построения динамической многоточечной сети DMVPN [3]. Для рассматриваемого в статье случая присутствуют два облака сети DMVPN с возможностью резервирования передаваемого трафика и создания динамических туннелей между spoke-маршрутизаторами с использованием протокола динамической маршрутизации OSPF. Техноло-

гия сети DMVPN подразумевает использование многоточечного GRE туннеля (mGRE) и протокола определения следующего транзитного узла (NHRP) [2] в связке с протоколами IPSec. Если данная технология не используется, шифрованный туннель не инициируется до того момента, пока отсутствует поток данных. Может потребоваться от 1 до 10 секунд для завершения инициирования туннеля IPSec, в это время отбрасывается поток данных. При использовании GRE с IPSec, настройка GRE туннеля включает в себя адрес назначения, который равноправно является адресом назначения IPSec. Туннели GRE и IPSec не информируют центральный узел о состоянии конфигурации удаленного узла в DMVPN сети. Узел сообщает о состоянии законченности конфигурации туннеля GRE с помощью протокола определения следующего транзитного узла NHRP. При включении удаленного узла автоматически инициируется туннель IPSec с центральным узлом. В случае использования NHRP удаленный узел уведомляет центральный узел о состоянии физического интерфейса и сообщает IP адрес. Использование данного протокола обязательно в следующих случаях:

– если IP адрес физического интерфейса назначен автоматически, то центральный узел не имеет возможность конфигурации для связи с удаленным узлом, т. к. при каждой перезагрузке удаленного узла изменяется IP адрес на его интерфейсе;

– конфигурация настройки упрощается, если информация о доступных удаленных узлах передается не через туннели GRE или IPSec, а динамически через NHRP;

– при добавлении нового удаленного узла в сеть DMVPN не требуется смена настройки центрального узла и каких-либо сторонних удаленных узлов. Создание и регистрация нового узла на центральном узле происходит динамически. Динамический протокол маршрутизации рассылает информа-

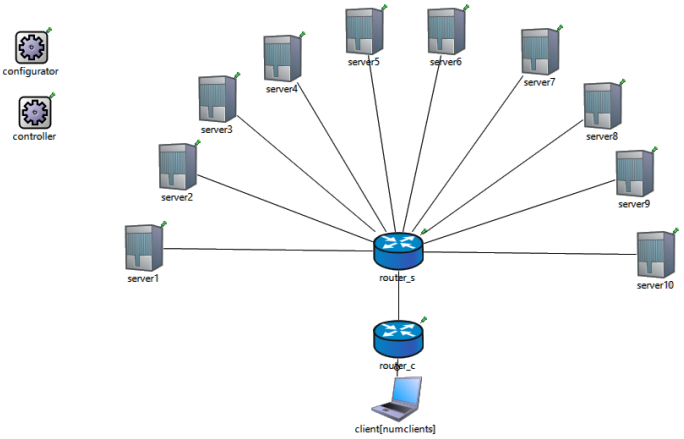

Рисунок 1. Модель множественных подключений с маршрутизацией

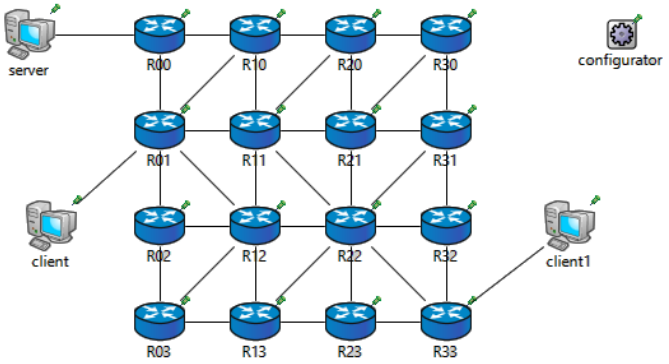

Рисунок 2. Модель многопутевого распределения информации

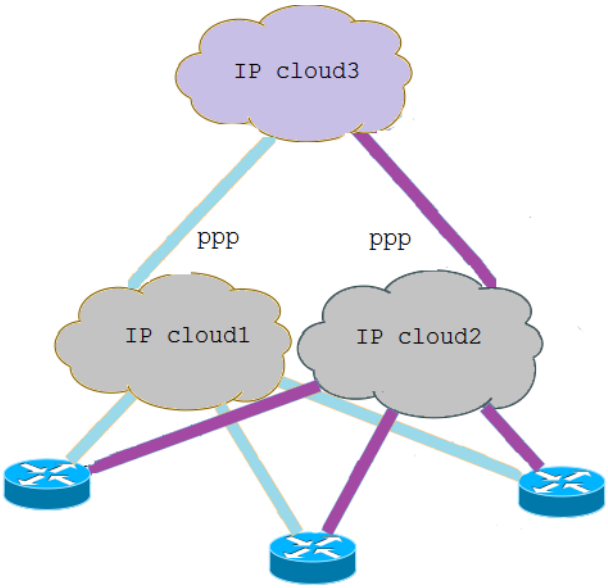

Рисунок 3. Общая модель VPN сети

цию о маршрутизации этого удаленного узла центральному узлу, а тот в свою очередь рассылает другим удаленным узлам информацию о маршрутизации.

В DMVPN сети все соединения идут от удаленных узлов к центральному, являются продолжительными и относительно постоянными. Удаленный узел использует протокол NHRP для определения адреса получается удаленного узла, если он хочет передать ему информацию. Два узла динамически создают IPSec туннель между собой через один интерфейс mGRE, после чего становится возможна передача данных. Динамический туннель автоматически разъединяется после определенного периода неактивности.

В настоящее время не придумано стандарта для передачи многоадресного или широковещательного IP пакета через IPSec туннель, из-за этого пакеты протокола динамической маршрутизации IP не могут передаваться через туннель IPSEC и любые изменения в маршрутизации нельзя распространить к другому концу IPSec туннеля. Туннели GRE реализованы на оборудовании Cisco с использованием виртуального интерфейса (interface tunnel). Протокол туннелирования разработан для обработки многоадресного или широковещательного IP пакета, как следствие, работа протокола динамической маршрутизации может быть выполнена по туннелю GRE. После этого становится возможным использования туннеля IPSec для шифрова туннельного пакета GRE.

При работе IPSec в транспортном режи существует ограничение на то, что пакет точника и получателя будет зашифрован т ко в том случае, когда адреса маршрутизато объявлены взаимно. Другими словами, ко ная точка GRE туннеля и одноранговые IP адреса будут одинаковыми. При использова обоих туннелей появляется возможность менять динамические протоколы маршрут ции для обновления таблиц маршрутизаци обоих концах зашифрованного туннеля. Пот трафика в данной модели показаны на рису 5 синими стрелками. Данные идут от кажд узла к каждому, т. е. применяется полносвяз full-mesh топология.

После тестирования модели были получены следующие результаты, представленные на рисунке 6:

Тот же трафик в пакетах в секунду представлен на рисунке 7:

В случае отказа связи облака №2 и облака №3 трафик между облаком №1 и облаком №3 возрастает:

Полученные результаты говорят о том, что в полносвязной топологии нагрузка на остальные связи возрастает в случае, когда какая-либо из связей перестаёт работать. Эти же результаты получаем относительно задержек до и после выхода линии из строя. Задержки при перемаршрутизации, как видно из рисунка 9, после

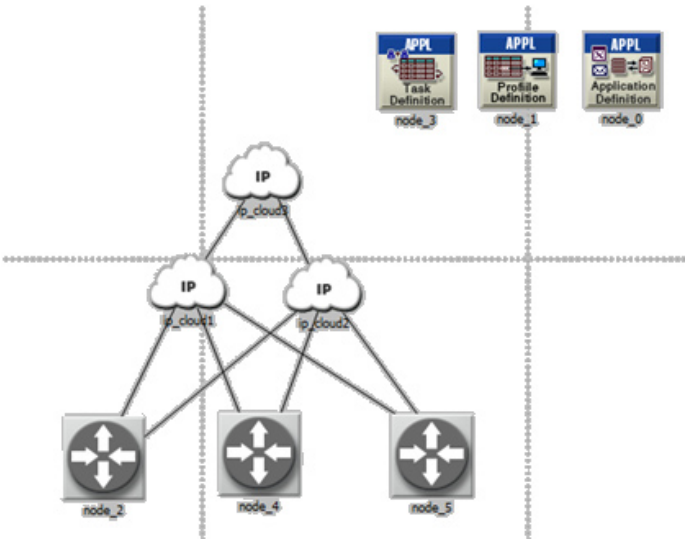

Рисунок 4. Схема VPN сети в Riverbed Modeler

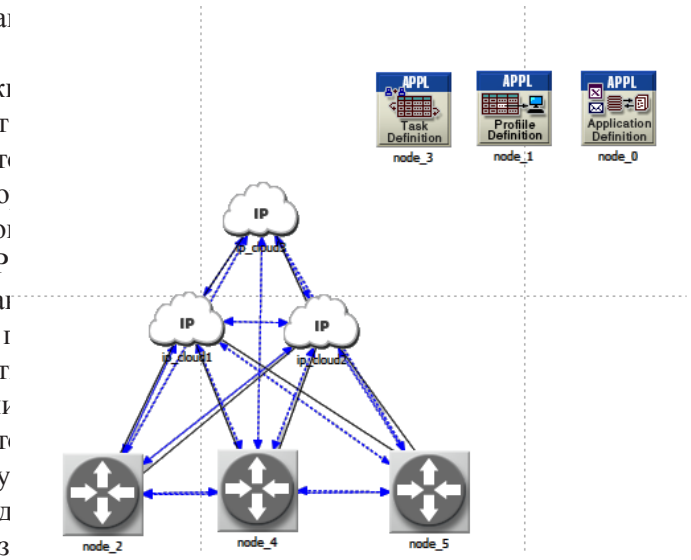

Рисунок 5. Модель трафика в сети

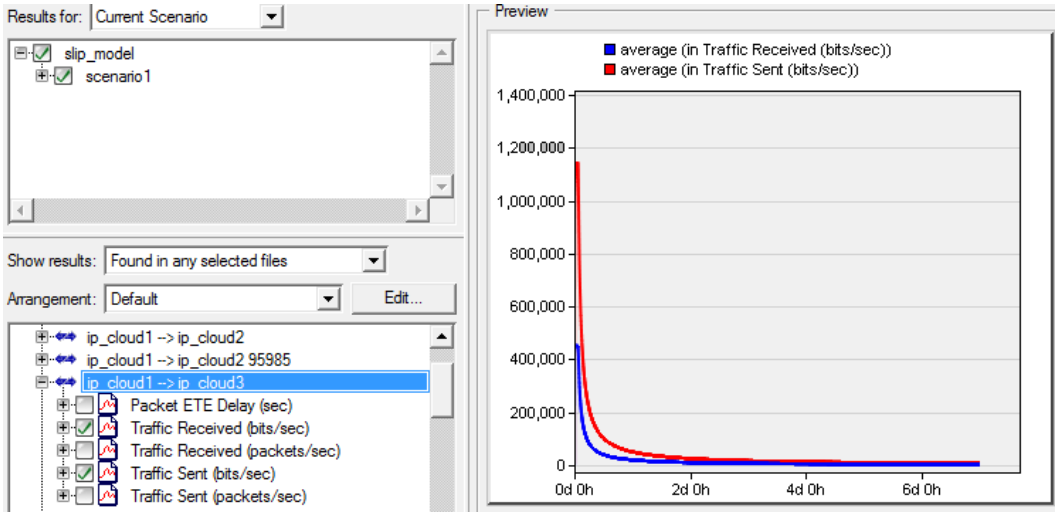

Рисунок 6. Результаты работы для фонового трафика

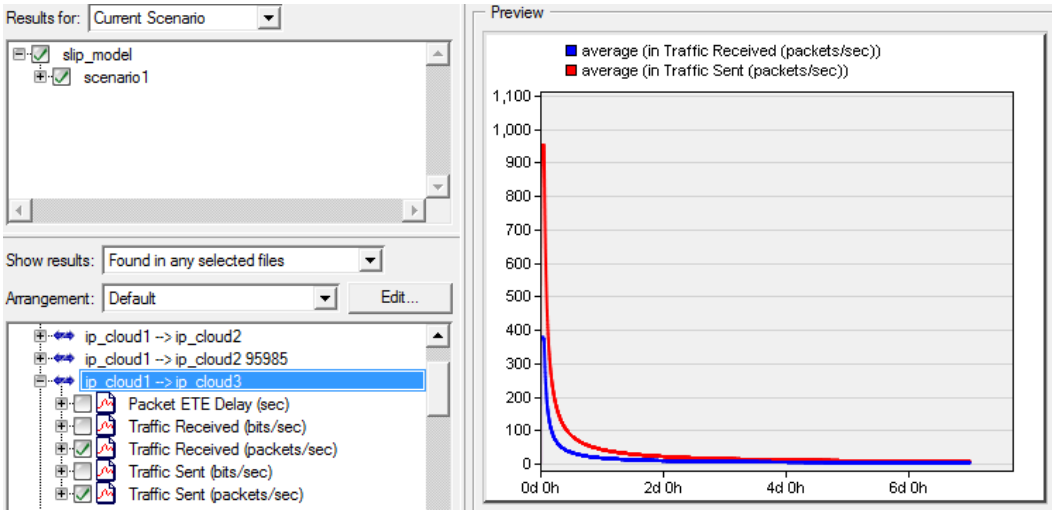

Рисунок 7. Результаты работы в пакетах/с

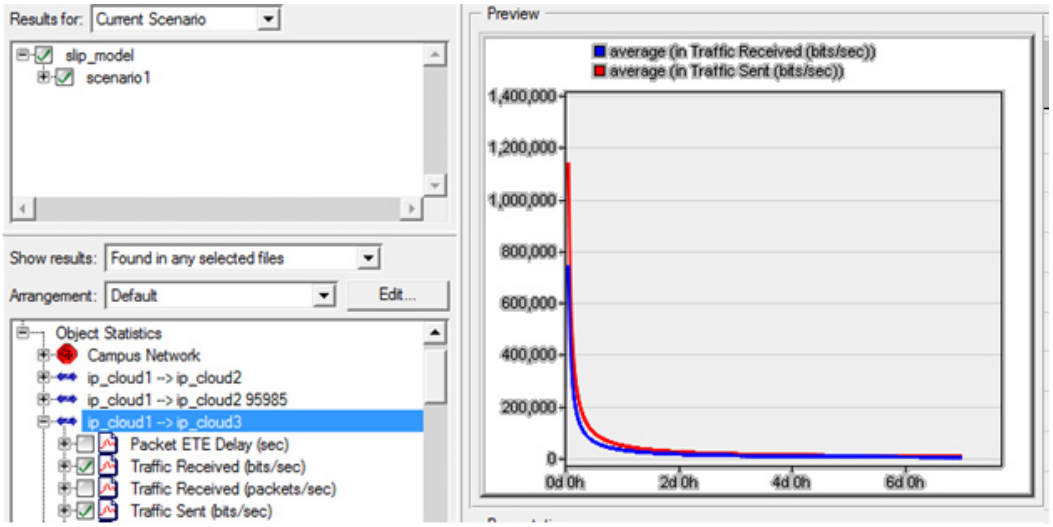

Рисунок 8. Результат работы при отказе связи

запуска всех протоколов невелики, и составляют не более одной секунды.

После смены маршрута для трафика принципиально ничего не изменилось:

Разработанная имитационная модель позволяет проводить эксперименты на любых топологиях, изменяя связность сети (рисунок 11) и параметры генерации сетевого трафика. Данная модель была перенесена в среду OMNET++ для

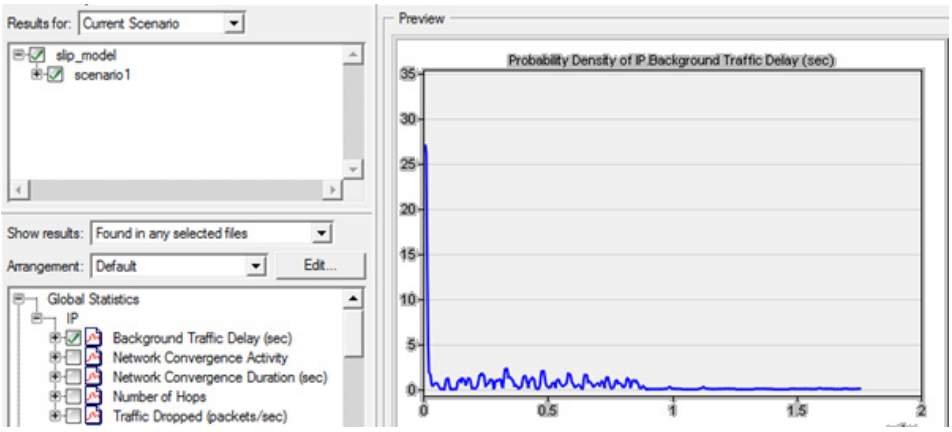

Рисунок 9. Задержки в линии

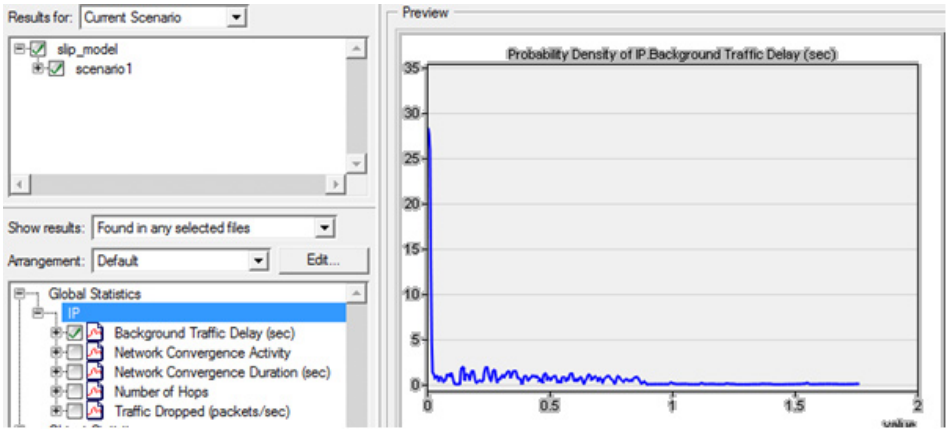

Рисунок 1, Задержки в линии после переключения маршрута

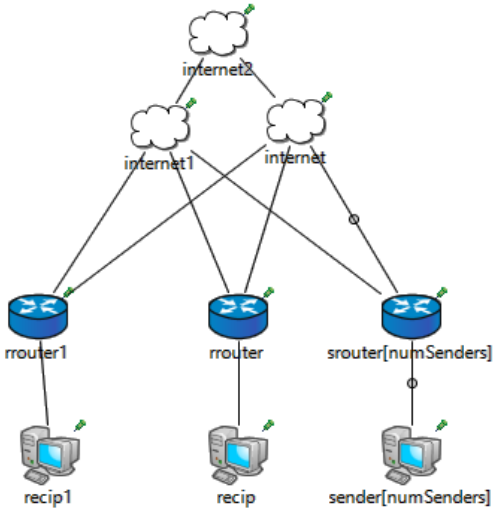

Рисунок 11. Модель сети в OMNET++

возможности более тонкой настройки и подключения модулей OpenFlow.

Облака internet и internet1 созданы по модели с рисунка 2, которая модифицирована под конкретные задачи, облако internet2 создано по модели с рисунка 1. Имитационную модель можно использовать в дальнейшем для построения симулятора сегмента сети. Симулятор позволит проводить тестирования с реальными контроллерами трафика OpenFlow и модельными устройствами.

Выводы

В результате исследования была описана имитационная модель самоорганизующейся частной виртуальной сети. В результате тестирования была выявлена зависимость возрастания нагрузки сети в случае отказа связи между узлами. Имитационная модель сети VPN может быть использована для проведения экспериментов на любых топологиях, а также для разработки симулятора сегмента сети.

10.11.2015

Исследования выполнены при поддержке РФФИ и правительства Оренбургской области (проекты №15-47-02686 и №14-07-97034), Президента Российской Федерации, стипендии для молодых ученых и аспирантов (СП-2179.2015.5)

Список литературы:

1. Ушаков Ю.А., Полежаев П.Н., Шухман А.Е. Создание мультисервисной многоточечной VPN сети с динамической автонастройкой // Вестник Оренбургского государственного университета. – 2015. – №9 (184). С. 170-178.
2. Полежаев П.Н., Бахарева Н.Ф., Шухман А.Е. Разработка эффективного генетического алгоритма маршрутизации и обеспечения качества обслуживания для программно-конфигурируемой сети. // Вестник Оренбургского государственного университета. – 2015. – №1 (176). С. 213-217.
3. Dynamic Multipoint VPN [Электронный ресурс] // Cisco Systems. Электрон. дан. — 2014. Режим доступа : http://www.cisco.com/c/en/us/products/security/dynamic-multipoint-vpn-dmvpn. (Дата обращения: 12.09.2015).
4. NHRP [Электронный ресурс] // Cisco Systems. ? Электрон. дан. — 2014. Режим доступа : http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html. (Дата обращения: 12.09.2015).

Сведения об авторах:

Ушаков Юрий Александрович, доцент кафедры геометрии и компьютерных наук Оренбургского государственного университета, кандидат технических наук, доцент
460018, г. Оренбург, пр-т Победы, 13, ауд. 1502, тел.: (3532) 372539, e-mail: unpk@mail.ru

Коннов Андрей Леонидович, доцент кафедры управления и информатики в технических системах Оренбургского государственного университета, кандидат технических наук, доцент
460018, г. Оренбург, пр-т Победы, 13, ауд. 1203, тел.: (3532) 37258, e-mail: andrey_konnov@mail.ru

Полежаев Петр Николаевич, преподаватель кафедры компьютерной безопасности и математического обеспечения информационных систем Оренбургского государственного университета
460018, г. Оренбург, пр-т Победы, 13, ауд. 20520, тел.: (3532) 372534, e-mail: peter.polezhaev@mail.ru

Шухман Александр Евгеньевич, заведующий кафедрой геометрии и компьютерных наук Оренбургского государственного университета, кандидат педагогических наук, доцент
460018, г. Оренбург, пр-т Победы, 13, ауд. 1502, тел.: (3532) 372539, e-mail: shukhman@gmail.com