УДК 621.391

АНАЛИЗ ИСТОЧНИКОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ VPRN НА БАЗЕ СЕТИ MPLS

Р.А. Бельфер[1], **И.С. Петрухин**[2]

[1]МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: a.belfer@yandex.ru;

[2]ЗАО "Российская Корпорация Средств Связи", Москва, Российская Федерация
e-mail: petrukhin@pkcc.ru

Ведущими провайдерами услуг большинство виртуальных частных сетей строятся как VPRN, т.е. на базе сетей MPLS. Это объясняется их преимуществом перед VPN на базе протокола IPSec — обеспечивают пользователям затребованное ими качество обслуживания соединения, обладают большей масштабируемостью, более эффективно используют пропускную способность сети и др. Опыт авторов настоящей работы по проектированию и вводу в эксплуатацию сетей VPRN показал актуальность проведения анализа обеспечения их информационной безопасности на всех трех плоскостях — управление сетью, управление соединением, работа конечного пользователя (данные). Для разных корпоративных сетей VPRN характерны определенные схемы взаимодействия виртуальных частных сетей в окружающей среде с устройствами других зон сети (топологии VPRN). Приведены результаты исследований уязвимости информационной безопасности к угрозам внедрения и атакам DoS злоумышленника в наиболее характерных шести топологиях корпоративных сетей VPRN. Приведены источники нарушения информационной безопасности. Показано, что некоторые потенциальные угрозы имеют место в эксплуатируемых сетях VPRN. Предложен реализованный в некоторых корпоративных сетях VPRN механизм защиты от таких угроз.

Ключевые слова: виртуальная частная сеть, информационная безопасность, таблица маршрутизации VPN; виртуальные частные маршрутизируемые сети, многопротокольная коммутация по меткам, отказ в обслуживании, центр управления.

ANALYSIS OF SOURCES OF INFORMATION SECURITY THREATS TO MPLS-BASED VPRNS

R.A. Bel'fer[1], **I.S. Petrukhin**[2]

[1]Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: a.belfer@yandex.ru;

[2]Russian Telecom Equipment Company, Moscow, Russian Federation
e-mail: petrukhin@pkcc.ru

The leading Internet-service providers build the majority of virtual private networks as virtual private routed networks (VPRNs), i.e., based on multipleprotocol label switching (MPLS) networks. This decision is preferred over IPSec-based VPNs because of advantages of VPRNs in flexibility of quality-of-service, scalability, effectiveness of bandwidth usage, etc. The experience in VPRN designing and putting into operation has shown that analysis of information security threats should be conducted in all three security planes: network management, connection (signaling) control, end user activities (data). Certain schemes of interaction of virtual private networks in the environment with devices of the other network areas (VPRN technologies) are characteristic of different corporative VPRNs. The results

of studying the information-security vulnerability to penetration threats and denial-of-service attacks of a trespasser are presented for six most characteristic corporative VPRN topologies. Sources of the information security violation are given. It is shown that some probable threats take place in the operated VPRNs. A mechanism implemented in the certain corporative VPRNs for protection against these threats is offered.

Keywords: virtual private network, information security, VPN routing table, virtual private routed networks, multipleprotocol label switching, denial of service, control center.

В работе [1] приведено сравнение основных технологий построения виртуальных частных сетей VPN на базе туннеля с помощью протокола IPSec и на основе многопротокольной коммутации по меткам (MPLS, Multiple Protocol Label Switching). При этом указано, что уровень безопасности в обеих технологиях VPN одинаково высокий. Это можно объяснить тем, что проводится сравнение только магистральных сетей VPN. В настоящей работе анализу подлежат уязвимости сетей VPN на базе MPLS на всех путях соединения, с учетом возможных источников угроз при взаимодействии с окружающей средой. Следует отметить, что большинство крупных провайдеров связи предпочитают строить сети VPN на базе MPLS. Несомненно, этому способствуют такие важные преимущества перед сетями VPN на IPSec, как обеспечение пользователям затребованного качества обслуживания соединения (точнее, класса обслуживания), бóльшая масштабируемость, более эффективное использование пропускной способности сети и др. [2].

Сети VPN на базе третьего уровня MPLS для отличия от сетей VPN второго уровня, выполненных на основе MPLS, часто называют виртуальными частными маршрутизируемыми сетями — VPRN (Virtual Private Routed Network). В настоящей статье такие сети будем называть просто VPN.

Одной из характеристик угроз информационной безопасности (ИБ) является описание источника угроз. Все эти угрозы могут исходить из разных источников: из самих сетей VPN, из сети Интернет, от провайдера услуг и др. Угрозы могут различаться по способу воздействия на VPN: вторжение, отказ в обслуживании — DoS (Denial of Service). Для проведения анализа возможных источников угроз ИБ в сетях VPRN необходимо определить архитектуру ИБ и возможные топологии сетей, определяющие среду взаимодействия сетей VPRN.

Архитектура ИБ VPRN. В архитектуру ИБ сети связи входит понятие плоскости безопасности (Security Plane), под которой понимается определенная функция сети связи, защищенная определенным способом. В рекомендации [3] по общим положениям архитектуры сетей связи определено 3 типа плоскости безопасности.

1. Плоскость безопасности (Management Security Plane) по управлению сетью, к которой относится защита функций администрирования,

эксплуатации и обслуживания сети OAM&P (Operation Administration Maintenance&Provision). В некоторых работах этот центр управления называется NOC (network operation center).

2. Плоскость безопасности (Control Security Plane) по обеспечению безопасности управления соединением, к которой относится защита функций и передаваемой по сети информации, например, по маршрутизации сообщений. Согласно документу [4], в сети VPRN сообщения протоколов LDP, BGP по обеспечению маршрутизации должны быть аутентифицированы. В этом документе в качестве механизма защиты рекомендуется протокол аутентификации MD5.

3. Плоскость безопасности конечного пользователя (End-User Security Plane). Плоскость безопасности конечного пользователя относится к безопасности сети доступа и пользования абонентами сетью поставщика услуг. К этой плоскости безопасности относится также защита потоков данных конечного пользователя. В документе [4] эта плоскость безопасности называется плоскостью безопасности данных (data plane). Под этим понимается защита от случаев нарушения политики безопасности, когда пакеты данной сети VPN поступают в другие сети VPN или наоборот.

Согласно работе [5], сформулированы следующие общие требования к информационной безопасности VPRN: разделение плоскости управления соединением (маршрутная изоляция), адресная изоляция от различных VPN, разделение пользовательских данных разных VPN и их пользователей, защита от атак DoS и спуфинга, аутентификация доступа.

Топологии сетей VPRN и источники угроз ИБ. В настоящем разделе приведены различные топологии взаимодействия виртуальных частных сетей с анализом источников угроз ИБ. К плоскости безопасности управления сетью относятся последние две из приведенных топологий. Остальные топологии относятся к плоскости безопасности управления соединением и плоскости безопасности конечного пользователя. На рис. 1 приведена топология взаимодействия сети VPRN с одним ядром MPLS. Здесь сеть VPN A состоит из двух сайтов, сеть VPN B — из трех сайтов и сеть VPN C — из четырех сайтов.

Показано, что ядро сети MPLS включает в себя внутренние маршрутизаторы провайдера P (Provider router) и граничные маршрутизаторы провайдера PE (Provider Edge router). Граничный маршрутизатор клиента CE (Customer Edge router) является оборудованием абонентского доступа к ядру сети MPLS. Для приведенной базовой модели безопасности недопустимо передавать сообщения из одной сети VPN в другую, из сети VPN — абонентам ядра сети (не в VPN), принимать в сети VPN сообщения от абонентов ядра сети. На практике модель безопасности более сложная, чем приведенная базовая модель. Например,

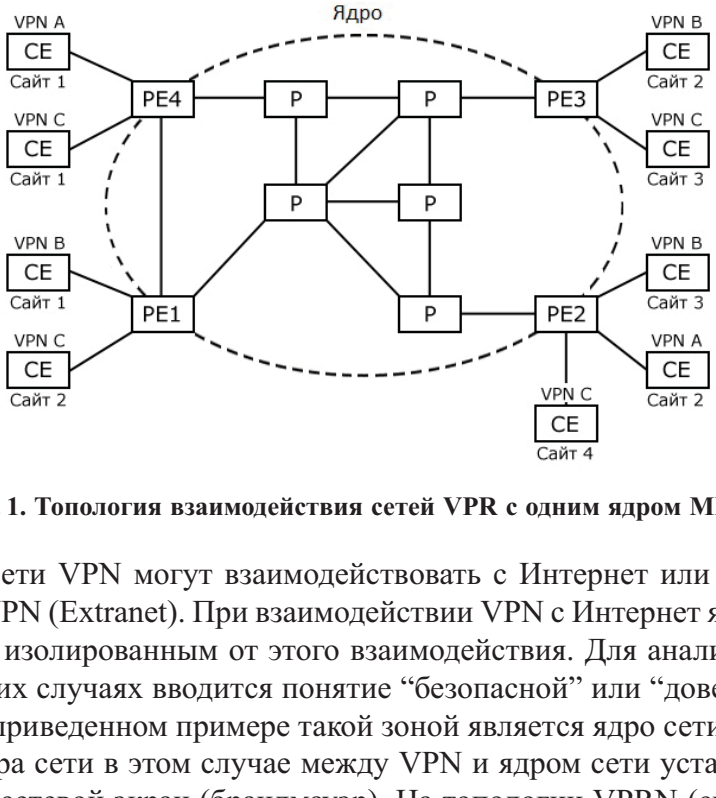

Рис. 1. Топология взаимодействия сетей VPR с одним ядром MPLS

многие сети VPN могут взаимодействовать с Интернет или другими сетями VPN (Extranet). При взаимодействии VPN с Интернет ядро сети остается изолированным от этого взаимодействия. Для анализа угроз ИБ в таких случаях вводится понятие “безопасной” или “доверенной” зоны. В приведенном примере такой зоной является ядро сети. Для защиты ядра сети в этом случае между VPN и ядром сети устанавливается межсетевой экран (брандмауэр). На топологии VPRN (см. рис. 1) приведем примеры, когда источником угроз является ответственный за формирование (конфигурирование) таблицы маршрутизации в PE. В результате установки нелегитимной команды таблицы маршрутизации VRF сайт одной VPN становится принадлежащей сайту другой сети VPN. Чрезмерно большое число запроектированных маршрутов через таблицу маршрутизации VRF может привести к атаке DoS (отказ в обслуживании). Покажем в качестве примера одну из возможных угроз в результате неправильного конфигурирования таблицы VRF.

При конфигурировании в PE каждой таблицы VRF задаются два атрибута маршрутной цели RT (Rout Target): один для определения политики EXPORT, а другой для определения политики IMPORT маршрутов. Как показано на рис. 2, при правильном конфигурировании таблица VRF сети VPN A устанавливает значения атрибутов RT (EXPORT и IMPORT), одинаковые и равные WHITE, а таблица VRF сети VPN B — также одинаковые значения атрибутов RT, но равные GREY [6]. Кроме RT для каждой таблицы VRF устанавливаются значения 64-битового разделителя маршрута RD (Route Distinguisher). В результате на маршрутизаторе PE все адреса, относящиеся к разным сетям VPN, будут различными, даже если они имеют одинаковые префиксы IP-сети. Для установления возможности передачи сообщений от пользователей сайта 2 пользователям сайта 1 VPN A по протоколу

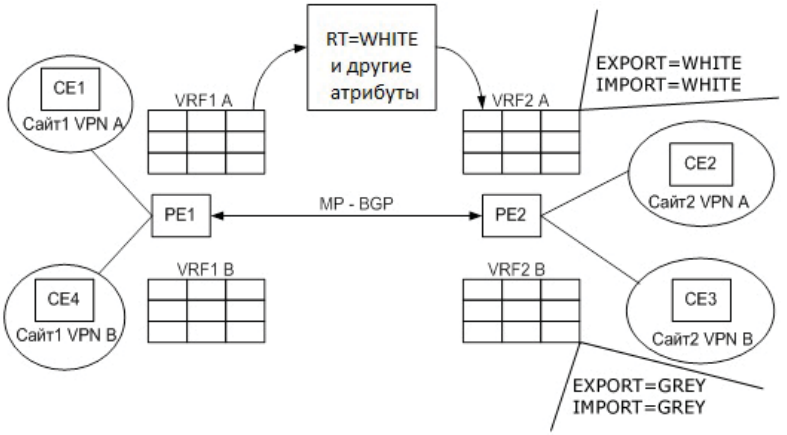

Рис. 2. Формирование таблицы маршрутизации

MP-BGP передается показанное на рис. 2 сообщение, включающее в себя атрибуты, в том числе атрибуты RT [7]. Сравнение значений атрибутов RT в этом сообщении и в установленных VRF позволяет решить вопрос о принятии или отклонении предлагаемого маршрута, что, в свою очередь, позволяет формировать топологию сети VPN. Маршрутизатор PE2 проверяет значение атрибута RT (политика экспорта — WHITE) в этом сообщении на совпадение с политикой импорта всех своих таблиц VRF (VRF2 A и VRF2 B). Атрибут RT WHITE совпадает с таблицей импорта VRF2 A, но не совпадает с таблицей импорта VRF2 B (GREY). Поэтому пакеты сайта 1 VPN A в рассмотренном случае корректного конфигурирования VRF будут приниматься только клиентами сайта 2 VPN A и не приниматься клиентами сайта 2 VPN B. Такая топология, когда значения политики экспорта и импорта определенной сети VPN, которая рассматривается в настоящем примере, называется полносвязной, т.е. каждый сайт может посылать пакеты непосредственно сайту, в котором находится сеть назначения. Теперь рассмотрим один из примеров некорректного конфигурирования VRF.

При получении от PE1 сообщения сайта VPN A маршрутизатор PE2 проверяет значение атрибута RT WHITE в этом сообщении на совпадение с политикой IMPORT всех своих таблиц VRF (VRF2 A и VRF2 B). Значение атрибута RT WHITE совпадает с RT WHITE политики IMPORT таблицы VRF2 A той же VPN A, но не совпадает с RT GREY политики IMPORT таблицы VRF2 B другой VPN (VPN B). Поэтому пакеты сайта 1 VPN A будут приниматься только клиентами сайта 2 VPN A и не будут приняты клиентами сайта 2 VPN B. Если злоумышленник при конфигурировании таблицы VRF сети VPN B установит одинаковые значения атрибуты RT, не равные GREY, а равные WHITE, то от сайта 1 VPN A будут поступать пакеты данных

не только на сайт 2 VPN A, но и в нарушение ИБ на сайт 2 VPN B. В приведенном примере такое нарушение обнаружится быстро. Однако, как отмечается в работе [8], существуют другие потенциальные некорректные варианты конфигурирования VRF с серьезными последствиями для ИБ VPN и некоторые из них очень трудно обнаружить.

Для приведенной на рис. 1 топологии VPRN отметим еще два источника угроз ИБ: граничные маршрутизаторы CE или PE. На участке абонентской линии CE–PE злоумышленник (пользователь VPN) может обманным способом получить легитимные адреса других пользователей этой же VPN и использовать их для передачи им незашифрованных данных на этом участке. Защитой от такой угрозы может быть шифрование/дешифрование данных пользователя на участке CE–CE. В работах [9–11] в качестве такого механизма предлагается использовать протокол IPSec [12]. В работе [13] предлагается алгоритм этого механизма. При этом защите подлежит весь путь между CE, включающий в себя каналы доступа (между CE и PE) и ядро MPLS (граничные маршрутизаторы, маршрутизаторы провайдера и каналы связи между ними). Этот же механизм обеспечивает защиту от перехвата данных на этом участке. При этом следует отметить, что наиболее критичной к такой угрозе ИБ является часть этого участка — абонентская линия (между CE и PE) и менее критичной — участки ядра сети.

Отметим также некоторые другие потенциальные угрозы ИБ на участке CE–CE при отсутствии шифрования:

- вставка фиктивных пакетов в VPN;
- изменение содержания пакета.

На рис. 3 приведен пример топологии взаимодействия VPRN с двумя ядрами MPLS [14]. Каждое ядро является автономной системой AS (Autonomous System) и обслуживается разными провайдерами услуг.

Взаимодействие между AS осуществляется через граничные маршрутизаторы автономной системы ASBR (Autonomous System Border routers). Здесь имеет место взаимодействие сайтов VPN между собой через два ядра сети MPLS.

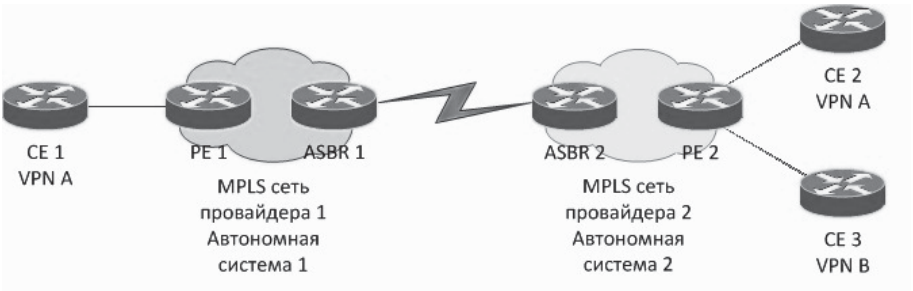

Рис. 3. Топология взаимодействия VPRN с двумя ядрами MPLS

Поскольку туннель LSP строится от PE в AS 1 к PE в AS 2 с использованием системных адресов самих PE, то ASBR должны функционировать как обычные P маршрутизаторы, за исключением того, что они не будут добавлять свою транспортную метку на пути движения пакета.

С учетом указанной схемы возникает возможность реализации атаки: AS 1 может передавать трафик с любой меткой VPN в AS 2 (так как на ASBR метки не могут проверяться). Эта потенциальная атака на приведенной топологии сети реально остается на настоящий момент незащищенной. Для защиты от такой угрозы предлагается реализованный на практике в некоторых корпоративных VPRN механизм установления сессии между ASBR с использованием разделителя маршрута RD. Шифрование/дешифрование на участке CE–CE также защищает от указанных выше угроз.

На рис. 4 приведен пример топологии VPRN, включающей в себя взаимодействие с Интернет [15]. Как следует из рис. 4, угрозы вторжения могут исходить от других VPN (через CE VPN *B*, PE, CE VPN *A*), из сети Интернет (через PE, CE VPN *A*), из ядра сети MPLS (через PE, CE VPN *A*). Все эти угрозы направлены на одного, нескольких или всех пользователей VPN *A*. Угрозы из Интернет вызваны тем, что в некоторых сетях VPN, согласно [4], один или несколько сайтов могут получать доступ к Интернет через шлюз (возможно, межсетевые экраны или брандмауэры — firewall).

На рис. 5 приведена другая топология VPRN, включающая в себя взаимодействие с Интернет. Здесь отмечены источники, которые могут быть использованы злоумышленником для атаки DoS (отказ в обслуживании). Как следует из рис. 5, такими пунктами, которые могут быть использованы злоумышленником для угрозы отказ в обслуживании (DoS), являются — маршрутизатор провайдера PE, граничный маршрутизатор клиента CE, маршрутизаторы провайдера P, канал связи ядра сети и каналы связи доступа в Интернет. Нарушение злоумышленником работы в ядре MPLS канала связи или маршрутизатора P также может быть атакой DoS для пользователей сайтов VPN,

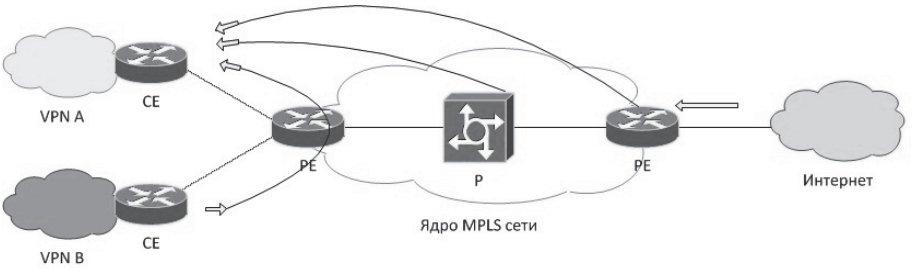

Рис. 4. Топология VPRN с источниками угроз вторжения

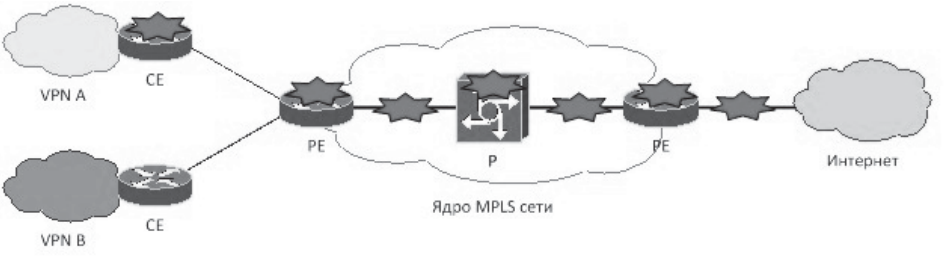

Рис. 5. Топология VPRN с источниками атак DoS

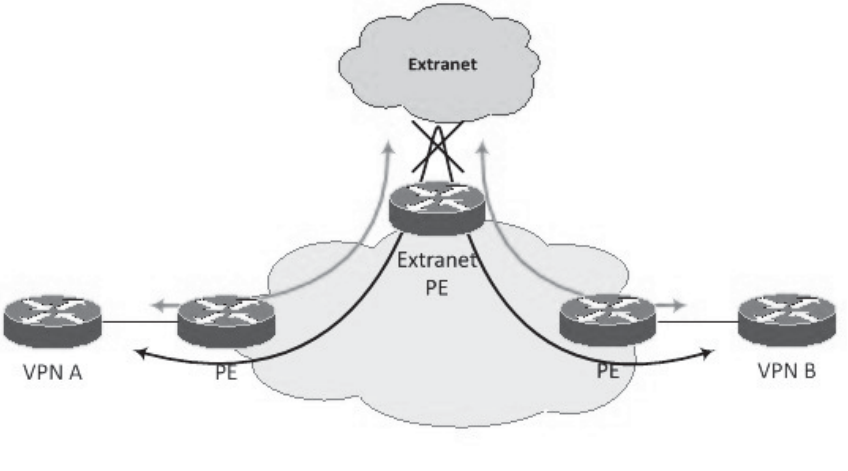

Рис. 6. Топология VPRN, включающая взаимодействие с Extranet

если через них маршрутизация пакетов осуществляется по меткам глобальной таблицы.

На рис. 6 приведена топология VPRN, включающая взаимодействие с общей инфраструктурой сети, называемой экстранет (extranet). С помощью атрибута маршрутной цели RT (один для определения политики экспорта, а другой — для определения импорта маршрутов сообщества) формируется топология VPN A и VPN B внутренней сети, VPN E внешней сети — extranet. Допустим, что такая топология, обеспечивает взаимодействие VPN A и VPN B только с VPN E. Источником угрозы для такой сети может быть намеренно некорректное конфигурирование таблиц маршрутизации в PE этих VPN (например, с помощью маршрутной цели RT). Последствием такой угрозы ИБ может быть создание нелегитимного взаимодействия между пользователями сайтов VPN A и VPN B.

На рис. 7 приведена топология VPRN, взаимодействующая с центром эксплуатации сети — NOC (Network Operation Center). Здесь показаны маршрутизаторы P и PE, подлежащие управлению из центра эксплуатации сети (NOC), а также каналы связи: внутриполосные каналы управления (in-band management channels), и внеполосные каналы

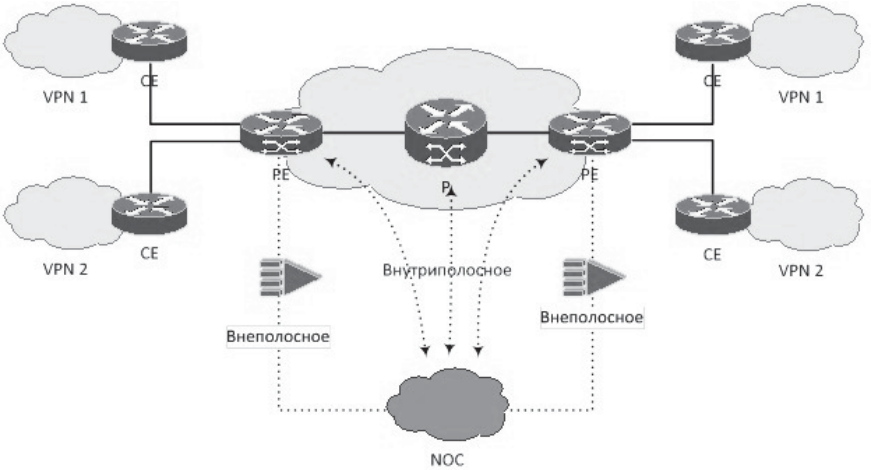

Рис. 7. Топология VPRN, взаимодействующая с центром эксплуатации сети (NOC)

управления (out-band management channels). Внутриполосные каналы управления соединяют NOC с маршрутизаторами не по IP-сети, а внеполосные каналы управления по IP-сети. Источниками угроз в такой топологии ИБ является NOC и указанные каналы связи управления, получившие нелегитимный доступ от злоумышленника.

Угрозы, направленные в NOC сети MPLS, представляют собой косвенные угрозы для VPRN. Центр NOC с точки зрения ИБ VPRN является одним из наиболее важных устройств, поскольку осуществляет управление всей сетью. Потенциально нарушение злоумышленником работы NOC может привести к большому риску ИБ VPRN. Источником атак на NOC могут быть все устройства и сети, подключенные к нему — внутренние маршрутизаторы P, граничные маршрутизаторы PE, граничными маршрутизаторы клиента CE, Интернет и др. На рис. 8 показана одна из разновидностей угроз, когда источником угроз для NOC является граничный маршрутизатор пользователя CE. Во многих сетях на участке PE–CE предусмотрено два логических канала, один из которых для VPN, а другой (внутриполосный) — для упра-

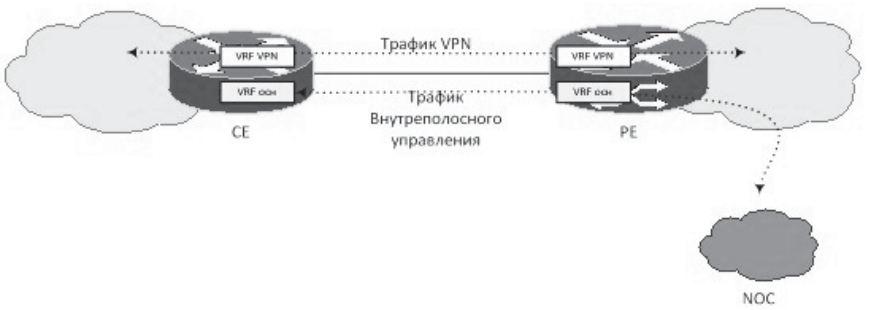

Рис. 8. Пример источника угроз CE в топологии VPRN на рис. 6

вления от NOC. Пользователи сайта CE, приведенного на рис. 8, через логический канал управления могут быть источником угрозы ИБ для NOC.

Выводы. Проведенный анализ источников угроз ИБ виртуальных частных маршрутизируемых сетей VPRN, краткое описание угроз, уязвимость ИБ при отсутствии защиты от некоторых из них позволяют использовать эти результаты на всех этапах обеспечения безопасности — при проектировании, испытаниях и эксплуатации корпоративных сетей связи.

ЛИТЕРАТУРА

1. *Оливейн В.* Структура и реализация современной технологии MPLS. М.: Вильямс, 2004. 480 с.
2. *Гольдштейн Ф.Б.*, *Гольдштейн Б.С.* Технология и протоколы MPLS. СПб.: БХВ-Петербург, 2005. 304 с.
3. *ITU-T Recommendation* X.805. Security architecture for system providing end-to-end communication, 2003.
4. *Rosen E.*, *Rekhter Y.* RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs), 2006.
5. *Luyuan Fang* [and others]. Interprovider IP-MPLS services: Requirements, implementations, and challenges // IEEE Communications Magazine. 2005. № 5. P. 119–128.
6. *Бельфер Р.А.* Сети и системы связи (технологии, безопасность): электронное учебное издание: МГТУ им. Н.Э. Баумана, 2012. 738 с.
7. *Олифер В.Г.*, *Олифер Н.А.* Компьютерные сети. СПб.: Питер, 2006. 997 с.
8. *Michael H. Behringer*, *Monique J. Morrow.* MPLS VPN security. Cisco Press, 2005. 312 с.
9. *Rong Ren*, *Deng-Guo Feng*, *Ke Ma*. A detailed implement and analysis of MPLS VPN based on IPSec // Proc. of the Third Int. Conf. on Machine Learning and Cybernetics. – Shanghai, 26–29 August 2004. P. 2779–2783.
10. *Mu Zhang*, *ZhongPing Tao*. Application research of MPLS VPN All-in-one campus card network based on IPSec 4th Int. Conf. on Computational and Information Sciences, 2012. P. 872–875.
11. *Jonah Pezeshki et al*. Performance implications of instantiating IPSec over BGP enabled RFC 4364 VPNS // IEEE, 2007. P. 1–7.
12. *Столлингс В.* Основы защиты сетей. Приложения и стандарты. М.: Вильямс, 2002. 324 с.
13. *Бельфер Р.А.* Угрозы безопасности VPN MPLS на участке между соседними маршрутизаторами и защита с помощью IPSec // Электросвязь. 2013. № 4. P. 25–27.
14. Bonica R., Rekhter Y., Raszuk R., Rosen E., Tappa D. CE-to-CE member verification for layer 3 VPNs. Available at: http://tools.ietf.org/id/draft-ietf-l3vpn-auth-00.txt (accessed: 28 February 2003).
15. Behringer M., Guichard J., Marques P. Layer 3 VPN import/export verification. Available at: http://tools.ietf.org/id/draft-ietf-l3vpn-vpn-verification-00.txt (accessed: 22 March 2005).

REFERENCES

[1] Oliveyn V. Struktura i realizatsiya sovremennoy tekhnologii [The structure and implementation of modern technologies MPLS]. Moscow, Vil'yams Publ., 2004. 480 p.

[2] Gol'dshteyn F.B., Gol'dshteyn B.S. Tekhnologiya i protokoly MPLS [Technology and MPLS protocols]. St. Petersburg, BKhV-Peterburg Publ., 2005. 304 p.
[3] ITU-T Recommendation X.805. Security architecture for system providing end-to-end communication, 2003.
[4] Rosen E., Rekhter Y. RFC 4364, BGP/MPLS IP virtual private networks (VPNs), 2006.
[5] Fang L. Interprovider IP-MPLS services: requirements, implementations, and challenges. *IEEE Commun. Mag.*, 2005, no. 5, pp. 119–128.
[6] Bel'fer R.A. Seti i sistemy svyazi (tekhnologii, bezopasnost'): elektronnoe uchebnoe izdanie [Networks and communication systems (technologies, security): electronic textbook]. Moscow, MGTU im. N.E. Baumana Publ., 2012. 738 p.
[7] Olifer V.G., Olifer N.A. Komp'yuternye seti [Computer networks]. St. Petersburg, Piter Publ., 2006. 997 p.
[8] Michael H.B., Monique J.M. MPLS VPN security. Cisco Press, 2005. 312 p.
[9] Rong Ren, Deng-Guo Feng, Ke Ma. A detailed implement and analysis of MPLS VPN based on IPSec. *Proc. 3d Int. Conf. Mach. Learn. Cybern.* Shanghai, 2004, pp. 2779–2783.
[10] Mu Zhang, ZhongPing Tao. Application research of MPLS VPN all-in-one campus card network based on IPSec, *4th Int. Conf. Comput. Inf. Sci.*, 2012, pp. 872–875.
[11] Pezeshki J. Performance implications of instantiating IPSec over BGP enabled RFC 4364 VPNS, *IEEE Proc.*, 2007, pp. 1–7.
[12] Stallings W. Network security essentials: applications and standards. Prentice Hall Press, 2001. 432 p. (Russ. ed.: Stollings V. Osnovy zashchity setey. Prilozheniya i standarty. Moscow, Vil'yams Publ., 2002. 324 p.).
[13] Bel'fer R.A. VPN MPLS security threats in the area between neighboring routers and IPSec protection. *Elektrosvyaz'* [Telecommunications], 2013, no. 4, pp. 25–27 (in Russ).
[14] Bonica R., Rekhter Y., Raszuk R., Rosen E., Tappa D. CE-to-CE member verification for layer 3 VPNs. Available at: http://tools.ietf.org/id/draft-ietf-l3vpn-auth-00.txt (accessed: 28 February 2003).
[15] Behringer M., Guichard J., Marques P. Layer 3 VPN import/export verification. Available at: http://tools.ietf.org/id/draft-ietf-l3vpn-vpn-verification-00.txt (accessed: 22 March 2005).

Статья поступила в редакцию 28.03.2013

Рувим Абрамович Бельфер — доцент кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор 92 научных работ в области информационных технологий.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

R.A. Bel'fer — assoc. professor of "Information Security" department of the Bauman Moscow State Technical University. Author of 92 publications in the field of information technologies.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russian Federation.

Илья Сергеевич Петрухин — инженер ЗАО "Российская Корпорация Средств Связи".
ЗАО "Российская Корпорация Средств Связи", Российская Федерация, 123242, Москва, пер. Капранова, д. 3, БЦ "Премьер Плаза".

I.S. Petrukhin — engineer of ZAO "Russian Telecom Equipment Company", Moscow, Russian Federation. Specializes in the field of information technologies.
ZAO "Russian Telecom Equipment Company", Premier Plaza Business Center, per. Kapranova, 3, Moscow, 123242 Russian Federation.