ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ VPN ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Ю. Николахин, *магистрант МТУСИ, 111024, г. Москва, ул. Авиамоторная, 8А, nexx1489@yandex.ru*

УДК 654.16

Аннотация. Рассмотрены основные технологии обеспечения безопасности при использовании *VPN* соединений. Рассмотрены и проанализированы основные протоколы *VPN*. Определены преимущества и недостатки отдельных протоколов и технологии в целом.

Ключевые слова: *VPN*; виртуальная частная сеть; безопасность; соединение; протоколы; удаленный доступ; общественные сети; передача информации; открытые каналы связи; шифрование.

THE USE OF VPN TECHNOLOGIES TO ENSURE INFORMATION SECURITY

Alexandr Nikolakhin, *master's student MTUCI, 111024, Moscow, ul. Aviamotornaya, 8A*

Annotation. The basic technologies of security when using *VPN* connections are considered. The main *VPN* protocols are considered and analyzed. The advantages and disadvantages of individual protocols and technology as a whole are identified.

Keyword: *VPN*; virtual private network; security; connection; protocols; remote access; public networks; information transfer; open communication channels; encryption.

В условиях все более глобализированной экономики компании начинают искать географическое распределение, либо связанное с налоговыми стимулами, либо просто с возможностью расширения. В этом случае сотрудники нуждаются в свободе осуществления своей деятельности без географических ограничений и безопасности передаваемой информации.

Концепция виртуальной частной сети, более известная как *VPN*, появилась как финансовая альтернатива защищенной коммуникации через общественные каналы связи, такие как интернет, и вскоре стала технологией, широко используемой услугой, ориентированной на безопасность, гарантирующей целостность, конфиденциальность и подлинность информации.

VPN не была первой технологией для удаленного подключения. Несколько лет назад наиболее распространенный способ подключения компьютеров между несколькими офисами состоял в использовании выделенной линии. Выделенные линии, такие как *ISDN* (цифровая сеть с интегрированными услугами, 128 Кбит/с), являются частными сетевыми соединениями, которые телекоммуникационная компания может арендовать для своих клиентов. Выделенные линии предоставили компании возможность расширить свою частную сеть за пределами ее непосредственной географической зоны. Эти соединения образуют единую глобальную сеть (*WAN*) для бизнеса. Хотя арендованные линии являются надежными, арендные договоры стоят дорого, при этом расходы растут по мере увеличения расстояния между офисами.

Сегодня интернет является более доступным, чем когда-либо прежде, и поставщики интернет-услуг (*ISP)* продолжают развивать более быстрые и надежные услуги при меньших затратах, чем выделенные линии. Чтобы воспользоваться этим, большинство предприятий заменили выделенные линии новыми технологиями, использующими интернет-соединения, не жертвуя производительностью и безопасностью. Предприятия начали с создания интрасетей, которые являются частными внутренними сетями, предназначенными для использования только сотрудниками компании. Интернет позволил удаленным коллегам работать вместе с помощью таких технологий, как совместное использование рабочего стола. Добавляя *VPN*, предприятия могут расширить ресурсы своей интрасети, позволяя сотрудникам работать в удаленных офисах или домах.

Цель *VPN* – обеспечить безопасное и надежное соединение между компьютерными сетями через существующую общедоступную сеть, как правило, интернет.

Хорошо спроектированная *VPN* предоставляет следующие преимущества:

- Расширенные соединения в разных географических точках без использования выделенной линии.
- Повышенная безопасность обмена данными.
- Гибкость для удаленных офисов и сотрудников при использовании интрасети через существующее интернет-соединение, как если бы они были напрямую подключены к сети.
- Экономия времени и средств.
- Повышенная производительность для географически распределенных ресурсов.

При этом от *VPN* всегда требуется:

- Безопасность. VPN должен защищать данные во время их движения в общедоступной сети. Если злоумышленники попытаются захватить данные, они не смогут их прочитать или использовать.
- Надежность. Сотрудники и удаленные офисы должны иметь возможность подключаться к *VPN* без каких-либо проблем, а *VPN* должен обеспечивать одинаковое качество соединения для каждого пользователя, даже когда он обрабатывает максимальное количество одновременных соединений.
- Масштабируемость. *VPN*-сервисы должны иметь возможность расширения.

Виртуальная частная сеть – это безопасный туннель между двумя или более компьютерами в интернете, позволяющий им получать доступ друг к другу, как в локальной сети. В прошлом *VPN*-сети в основном использовались компаниями для надежной связи удаленных филиалов или подключения роуминг-сотрудников к офисной сети, но сегодня они также являются важной услугой для потребителей, защищая их от атак при их подключении к общедоступным беспроводным сетям.

Открытые беспроводные сети представляют серьезную угрозу для пользователей, поскольку злоумышленники, сидящие в тех же сетях, могут использовать различные методы для отслеживания веб-трафика и даже захвата учетных записей на сайтах, которые не используют протокол безопасности *HTTPS*. Кроме того, некоторые операторы сетей *Wi-Fi* намеренно вводят рекламу в веб-трафик, что может привести к нежелательному отслеживанию.

В некоторых регионах мира правительства отслеживают пользователей, посещающих определенные веб-сайты, чтобы выявить их политическую принадлежность и определить диссидентов – практики, которые угрожают свободе слова и правам человека.

Используя VPN-соединение, весь трафик можно безопасно маршрутизировать через сервер, расположенный в другом месте в мире. Это защищает от локальных попыток отслеживания и взлома и даже скрывает реальный адрес интернет-протокола с веб-сайтов и служб, к которым происходит обращение.

Существуют различные технологии *VPN* с разной степенью шифрования. Например, протокол туннелирования «точка-точка» (*PPTP*) работает быстро, но гораздо менее безопасен, чем другие протоколы, такие как *IPSec* или *OpenVPN*, который использует *SSL/TLS* (Secure *Sockets Layer/Transport Layer Security*). Кроме того, при использовании *VPN* на основе *TLS* также важны тип алгоритма шифрования и длина ключа.

Хотя *OpenVPN* поддерживает множество комбинаций шифров, протоколов обмена ключами и алгоритмов хеширования, наиболее распространенной реализацией, предлагаемой поставщиками услуг *VPN* для соединений *OpenVPN*, является шифрование *AES* с обменом ключами *RSA* и сигнатурами *SHA*. Рекомендуемыми параметрами являются шифрование AES-256 с ключом *RSA* длиной не менее 2048 бит и криптографическая хэш-функция *SHA*-2 (*SHA*-256) вместо *SHA*-1.

Стоит отметить, что шифрование может влиять на скорость соединения. Выбор технологии VPN и методов шифрования должен производиться в каждом конкретном случае, в зависимости от того, какие данные будут передаваться.

VPN также используется для доступа к онлайн-контенту, который недоступен в определенных регионах, хотя это зависит от того, насколько хорошо владельцы контента применяют ограничения. Поставщики услуг *VPN* обычно запускают серверы во многих странах по всему миру и позволяют пользователям легко переключаться между ними. Например, пользователи могут подключаться через сервер одной страны для доступа к ограниченному содержимому в их собственной или другой стране.

Пользователи в таких странах, как Китай или Турция, где правительства регулярно блокируют доступ к определенным веб-сайтам по политическим причинам, обычно используют *VPN*, чтобы обойти эти ограничения.

При развертывании *VPN* на международном уровне необходимо убедиться, что законы и правила разных стран не нарушаются, поскольку там могут быть ограничены сервисы *VPN*. Примечательно, что Китай в начале этого года опубликовал правила *VPN*, которые являются неопределенными, но могут быть истолкованы как незаконные при использовании *VPN* на территории страны. Правила могут быть нацелены на потребителей, пытающихся посещать запрещенные веб-сайты, но они могут также применяться к предприятиям, подключающимся к филиалам в другом месте. В России также были предложения о запрете *VPN*, но пока они не нашли поддержки. Суть заключается в том, чтобы проверить законы в любых странах, где будет размещаться узел *VPN*, чтобы убедиться, что он является законным и существуют ли правила, которые могут подорвать конфиденциальность.

По мере увеличения разнообразия и интенсивности кибер-угроз сетевым администраторам необходимо сбалансировать стремление полностью заблокировать внутренние сети своей организации для доступа через интернет, одновременно необходимо обеспечить повсеместный доступ к внутренней сети из множества удаленных устройств, сотрудников, клиентов и *IoT*. Этот баланс может быть достигнут за счет использования виртуальной частной сети (*VPN*), которая использует интернет для обеспечения безопасного доступа к виртуальной сети.

Лучший способ защитить конфиденциальные данные и приложения – это ограничить доступ к ним через «общедоступные сети», такие как интернет. Сети, которые соединяют инфраструктуру, в которой хранятся конфиденциальные данные, изолированы от интернета, чтобы защитить их, используются IP-адреса, недоступные через интернет. Безопасность усиливается за счет ограничения доступа к этим сетям, поэтому доступ к ним может получить только определенный трафик только от авторизированных внешних устройств. Эти изолированные и ограниченные сети называются «частными сетями».

Предприятие может иметь частную сеть, которая связывает всю свою ИТ-инфраструктуру и компьютеры сотрудников с корпоративной интрасети. Эта сеть позволяет получить доступ ко всем внутренним ИТ-услугам, таким как зарплата, электронная почта и т. д. в главном офисе предприятия. По мере роста предприятия частная сеть также может быть расширена до дополнительных филиалов.

Для установления связи между офисами, для их частной сети при сохранении сети отдельно от интернета часто используется выделенный транспорт данных с арендованными линиями электросвязи. Телекоммуникационные услуги, используемые для создания этой связи между местоположениями, довольно дороги и необходимы более экономичные альтернативы.

Благодаря достижениям в области криптографии, вычислительной техники и интернета стало возможным шифровать трафик данных и туннелировать его через интернет на сервер, расположенный в частной сети. Защищенный туннель создает виртуальную связь, которая расширяет частную сеть через общедоступную сеть.

VPN может использовать одну из многих технологий, таких как безопасность протокола *IP (IPsec),* безопасность транспортного уровня *(SSL/TLS*), безопасность транспортного уровня данных (*DTLS*), безопасное подключение устройств или сетей через общедоступные сети, чтобы расширять или формировать частную сеть.

Та же технология, которая используется для создания виртуального соединения между сетями, также может использоваться для подключения устройств пользователя к частной сети. Общее использование *VPN* – это предоставление удаленным сотрудникам безопасного доступа через интернет к ИТ-услугам своей компании. Сотрудники используют *VPN*-клиентов, установленных на корпоративных ноутбуках или мобильных устройствах, для подключения к VPN-серверу, который присутствует в частной сети компании.

Случай использования удаленного доступа не ограничивается доступом для сотрудников. Любое устройство, подключенное к интернету, может использовать *VPN*, чтобы быть частью частной сети. Устройства могут варьироваться от обычных вычислительных устройств, таких как ноутбуки, до специализированных промышленных датчиков или бытовой электроники, таких как интеллектуальные телевизоры.

По мере того, как все больше устройств и служб подключаются к глобальной сети, степень опасности кибер-атак возрастает. *VPN*-доступ к необходимым устройствам позволяет снизить потенциальные угрозы. Правильно реализованная *VPN* позволяет только доверенным устройствам получать доступ к частной сети и внедрять строгие средства контроля доступа для обеспечения доступа с наименьшими привилегиями. Эти меры уменьшают количество атак, доступных хакерам, чтобы поставить под угрозу безопасность сети.

VPN-решения также обеспечивают взаимную аутентификацию, в которой как *VPN*-сервер, так и соединительное устройство аутентифицируют друг друга. При успехе пользователь, получающий доступ к сети, аутентифицируется с использованием имени пользователя/пароля и, необязательно, с использованием другой формы аутентификации, которая может быть маркером безопасности, например, с использованием мобильного телефона или смарт-карты. Как только устройство и пользователь аутентифицируются, *VPN*-сервер может применять правила доступа, чтобы пользователь получал доступ только к подмножеству систем/служб, к которым у него есть права доступа.

Другим преимуществом безопасности, которое обеспечивает использование *VPN,* является шифрование данных, что защищает от подслушивания и потери данных.

Сегодня набирает популярность применение *SaaS* сервисов. Которые также могут обеспечивать распределенное использование ресурсов.

Но не все приложения *SaaS* предлагают достаточно высокий уровень безопасности. Обычно приложения *SaaS* полагаются только на аутентификацию имени пользователя и пароля. Если не следовать рекомендациям по безопасности для защиты паролем и блокировки учетных записей при неудачных попытках, для получения несанкционированного доступа могут использоваться атаки и эксплойты с использованием грубой силы на слабых механизмах восстановления пароля. Поэтому разумно разрешить принудительные корпоративные политики безопасности с помощью *VPN* для подключения к корпоративной сети, а затем для доступа к приложениям *SaaS* через корпоративную сеть.

HTTPS, также не может рассматриваться в качестве альтернативы *VPN*. *HTTPS* не может постоянно использоваться во время всего сеанса веб-просмотра. Он обычно используется только на определенных сайтах и только для определенных транзакций, в которых передается конфиденциальная информация, такая как имя пользователя/пароль или информация о кредитной карте. *HTTPS* делает хорошую работу по защите конфиденциальной информации во время использования, но для обеспечения конфиденциальности всего сеанса просмотра вебстраниц и защиты всего трафика при подключении к ненадежным сетям лучше всего использовать *VPN*. *HTTPS* использует *TCP* и обеспечивает безопасность для веб-приложений. Таким образом, он не способен обеспечить трафик со всех не-веб-приложений, которые могут использоваться на устройстве, таких как электронная почта или *VoIP* и потоковые приложения, которые не полагаются на *TCP*, такие как *Skype* или *Spotify*. При использовании *VPN* весь трафик с устройства, независимо от приложения, генерирующего трафик, *можно* защитить. Будучи защищенным транспортным протоколом конкретного приложения*, HTTPS* не действует как виртуальная частная сеть и, следовательно, не может обеспечить все преимущества *VPN,* такие как доступ к общим папкам файлов, сетевым принтерам и другим сетевым ресурсам более крупной частной сети.

Основная цель *VPN* – обеспечить безопасный доступ к частной сети, не будучи напрямую подключенной к физической частной сети. Таким образом, *VPN* расширяет все сервисы, доступные в частной сети, как если бы устройства напрямую подключались к частной сети.

Корпоративные ИТ-специалисты могут предоставлять такие услуги, как файловые серверы, серверы печати, веб-сайты интрасети, системы *ERP*, серверы резервного копирования и т. д. Эти службы предназначены только для внутреннего использования, но с применением *VPN* сотрудник не ограничивается физическими местоположением и может иметь прямое подключение к внутренней ИТ-сети из любой географической точки.

Та же частная сеть может предоставлять специализированные услуги для подключенных к интернету устройств, таких как *IP*-телефония или управление устройствами. *VPN* можно использовать для безопасного подключения этих устройств к вычислительной инфраструктуре, которая предоставляет специализированные услуги по частной сети. *VPN* – отличное решение для безопасной передачи данных, передаваемых и полученных различными устройствами, которые включают в себя расширяющуюся область интернета вещей (*IoT*).

Необходимо также понимать, что риски безопасности*,* связанные с *VPN,* также существуют. К ним относятся захват *VPN*, в котором неавторизованный пользователь захватывает *VPN*-соединение с удаленного клиента, атаки *man-in-the-middle*, в которых злоумышленник способен перехватывать данные, слабую аутентификацию пользователя, разделенное туннелирование, в котором пользователь получает доступ к небезопасному подключению к интернету, а также доступ к *VPN*-подключению к частной сети, заражению вредоносными программами на клиентском компьютере, предоставлению слишком большого количества прав доступа к сети и утечке *DNS,* в которых компьютер использует *DNS*-соединение по умолчанию, а не защищенный *DNS*-сервер *VPN*.

Чтобы устранить эти риски, необходимо учитывать дополнительные функции безопасности *VPN* при выборе продукта *VPN*. К ним относятся обязательные функции безопасности:

- Поддержка надежной аутентификации.
- Надежные алгоритмы шифрования.
- Использование антивирусного программного обеспечения и средств обнаружения и предотвращения вторжений.
- Надежная защита по умолчанию для портов администрирования и обслуживания.
- Поддержка цифрового сертификата.
- Поддержка регистрации и аудита.
- Возможность назначать адреса клиентам в частной сети, при этом все адреса остаются закрытыми.

Кроме того, для администраторов сети и безопасности, а также для сотрудников службы поддержки и для удаленных пользователей необходимо провести обучение, чтобы они следовали лучшим передовым методам безопасности во время внедрения *VPN* и постоянного использования.

Еще один способ улучшить безопасность *VPN* – это совершенная прямая секретность (*PFS*). Если используется *PFS*, зашифрованные сообщения и сеансы, записанные в прошлом, не могут быть получены и дешифрованы, если скомпрометированы долгосрочные секретные ключи или пароли.

С *PFS* каждый сеанс *VPN* использует различную комбинацию ключей шифрования, поэтому даже если злоумышленники украдут один ключ, они не смогут расшифровать любые другие сеансы *VPN*.

Существует четыре основных типа *VPN*:

- *VPN*-брандмауэр оснащен как брандмауэром, так и *VPN*-возможностями. Этот тип использует защиту, предоставляемую брандмауэрами, для ограничения доступа к внутренней сети и обеспечивает перевод адресов, аутентификацию пользователя, аварийные сигналы и протоколирование.
- Аппаратная *VPN* обеспечивает высокую пропускную способность сети, а также улучшает производительность и надежность, но является дорогостоящей.
- Программный *VPN* обеспечивает гибкость с точки зрения управления трафиком. Это лучше всего, когда конечные точки не контролируются одной стороной и при использовании разных брандмауэров и маршрутизаторов.
- Безопасный уровень сокета (*SSL*) *VPN* позволяет пользователям подключаться к *VPN*-устройствам с помощью веб-браузера. *SSL* используется для шифрования трафика между веб-браузером и устройством *VPN*.

Протоколы туннелирования *VPN* предлагают разные функции и уровни безопасности, и для каждого из них есть преимущества и недостатки. Существует пять основных протоколов туннелирования *VPN*: Протокол туннелирования защищенных сокетов *(SSTP),* Протокол туннелирования «точка-точка» (PPTP), Протокол туннелирования второго уровня *(L2TP), OpenVPN* и *Internet Key Exchange* версии 2 *(IKEv2).*

- *SSTP* использует протокол *HTTPS* для передачи трафика через брандмауэры и веб-прокси, которые могут блокировать другие протоколы. *SSTP* предоставляет механизм для переноса трафика протокола «точка-точка» (*PPP*) по каналу *SSL*. Использование *PPP* позволяет поддерживать надежные методы аутентификации, а *SSL* обеспечивает безопасность на уровне транспорта с расширенным согласованием ключей, проверкой шифрования и целостности.
- *PPTP* позволяет зашифровать многопротокольный трафик и затем обернуть его в заголовок, который будет отправлен через сеть интернет-протокола (*IP*). *PPTP* можно использовать для удаленного доступа и *VPN*-соединений «точка-точка». При использовании интернета *PPTP*-сервер является *VPN*-сервером с поддержкой *PPTP* с одним интерфейсом в интернете и вторым интерфейсом в корпоративной интрасети. *PPTP* использует соединение протокола управления передачей для управления туннелями и инкапсуляции общей маршрутизации для переноса кадров *PPP* для туннелированных данных.
- *L2TP* позволяет зашифровать многопротокольный трафик, а затем использовать любой носитель, поддерживающий доставку данных PPP, например, IP или асинхронный режим передачи. *L2TP* – это комбинация *PPTP* и *Layer* 2 *Forwarding (L2F). L2TP* представляет лучшие функции *PPTP* и *L2F*. В отличие от *PPTP, L2TP* полагается на *IP*-безопасность (IPsec) в транспортном режиме для служб шифрования. Комбинация *L2TP* и *IPsec* известна как *L2TP / IPsec*. Оба *L2TP* и *IPsec* должны поддерживаться как клиентом VPN, так и *VPN*-сервером. *L2TP*/*IPsec* – идеальная передовая секретность.
- *OpenVPN* – это программное приложение с открытым исходным кодом, которое реализует методы *VPN* для создания безопасных соединений «точка-точка» или «сайт-сайт» в маршрутизированных или мостовых конфигурациях и средствах удаленного

доступа. Он использует собственный протокол безопасности, который использует *SSL/TLS* для обмена ключами. *OpenVPN* позволяет одноранговым узлам аутентифицировать друг друга с помощью секретного ключа, сертификата или имени пользователя и пароля. Большинство провайдеров *VPN*, использующих *OpenVPN*, используют прямую секретность.

- *IKEv*2 – это протокол на основе протокола *IPSec*, который используется в *Windows* 7 и выше. *IKEv*2 – это стандарт следующего поколения для безопасного обмена ключами между одноранговыми *VPN*-устройствами. *IKEv*2 особенно полезен в автоматическом восстановлении *VPN*-соединения, когда пользователи временно теряют свои интернет-соединения.

Какой *VPN* протокол является наиболее безопасным?

Несмотря на то, что он основан на открытых источниках, многие рассматривают *OpenVPN* как самый безопасный протокол *VPN*. Он стабилен и надежен, легко конфигурируется для работы на любом порту, поддерживает аппаратное ускорение для улучшения скорости, способен пересекать межсетевые экраны и трансляцию сетевых адресов (*NAT*) и использует библиотеки *OpenSSL* для шифрования. Однако он требует клиентского программного обеспечения и не может использоваться на *iPhone* и только на ограниченном количестве телефонов *Android*.

Другой защищенный протокол *VPN-L2TP/IPSec*. У него есть устойчивый алгоритм шифрования, никакое дополнительное программное обеспечение для устройств не требуется, он встроен в большинство настольных операционных систем и мобильных устройств, довольно легко реализовывается и не имеет известных серьезных уязвимостей. Тем не менее, у него есть проблемы с брандмауэрами, сложнее настроить на сервере *Linux* и относительно легко блокируется интернет-провайдерами.

SSTP обеспечивает надежное шифрование, его очень сложно обнаружить и заблокировать, он поддерживается на всех устройствах *Microsoft Windows*. В то же время он не поддерживается всеми поставщиками *VPN* и у него ограниченная поддержка устройств, отличных от Windows.

Наименее защищенный протокол *VPN* – это протокол *PPTP*. Его преимущества включают легкую настройку, широкую поддержку большинства устройств и низкие накладные расходы. Поскольку он существует уже давно, в нем имеются известные проблемы безопасности, которые могут быть использованы хакерами (или правительственными учреждениями). Он имеет слабое шифрование и относительно легко блокируется провайдерами.

*IKEv*2 поддерживается как часть реализации *IPSec* в *Windows,* прост в использовании. Однако ошибки разработчиков все еще встречаются, и проблема совместимости между различными поставщиками также существует.

Какой протокол *VPN* лучше зависит от предприятия и пользователя? Для тех, кто ищет наиболее безопасный, хорошим вариантом может быть *OpenVPN*. Для тех, кто ищет поддержку для многих устройств, *PPTP* может оказаться удачным решением.

VPN обеспечивает средства доступа к защищенной корпоративной сети через небезопасные общедоступные сети. В то время как *VPN* является улучшенной технологией по сравнению с передачей незашифрованных данных по сетям общего пользования, потенциальные недостатки безопасности должны учитываться пользователями, планирующими развертывание *VPN* или уже использующими эту технологию. Использование *VPN* значительно увеличивает безопасность каналов связи распределенных узлов.

Литература

1. URL https://computer.howstuffworks.com/vpn3.htm (дата обращения - октябрь 2018).

2. URL https://ostec.blog/en/general/secure-remote-access-vpn (дата обращения - октябрь 2018).
3. URL https://www.sans.org/reading-room/whitepapers/vpns/paper/881 (дата обращения - октябрь 2018).
4. URL https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-vpn/ (дата обращения - октябрь 2018).
5. URL https://www.esecurityplanet.com/network-security/vpn-virtual-private-network.html (дата обращения - октябрь 2018).
6. URL https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/ (дата обращения - октябрь 2018).
7. URL https://www.cisco.com/c/en/us/solutions/enterprise-networks/security/networking_solutions_products_genericcontent0900aecd8051f37b.html (дата обращения - октябрь 2018).
8. URL https://securityintelligence.com/is-corporate-vpn-security-dead/ (дата обращения - октябрь 2018).
9. URL https://www.finjanmobile.com/vpn-help-protect-privacy/ (дата обращения - октябрь 2018).
10. Браун, Стив Виртуальные частные сети / Стивен Браун; Пер.с англ. О. Труфанов. – М.: Лори, 2001. – XX, 508 с.
11. Росляков А.В. Виртуальные частные сети. Основы построения и применения. – М.: ЭКО-ТРЕНДЗ, 2006. – 300 с.
12. Ибе О. Сети и удаленный доступ: Протоколы, проблемы, решения: Пер.с англ. / Оливер Ибе. – М.: ДМК, 2002. – 332с.
13. Мезенцев А.В. Технологии защищенной обработки информации: учеб. пособие. / А.В. Мезенцев, Н. И. Синадский, Д. А. Хорьков; Федер. гос. бюджет. учреждение высш. проф. образования "Иркут. гос. ун-т", Ин-т математики, экономики и информатики. – Иркутск: Изд-во ИГУ, 2013. – 120 с.
14. Столлингс В. «Основы защиты сетей. Приложения и стандарты - М.: «Вильямс», 2012. – 432 с.
15. Колесников, О. Linux: создание виртуальных частных сетей (VPN) [Текст]: пер. с англ. / О. Колесников, Б. Хетч. – М.: КУДИЦ-Образ, 2004. – 459 с.