Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики и
информационных технологий

Организация защиты данных при их передаче в сети Интернет

АВТОРЕФЕРАТ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

студента 2 курса 271 группы
направления 09.04.01 «Информатика и вычислительная техника»
факультета компьютерных наук и информационных технологий
Абдулайми Мустафы Аббас Зейдана

Научный руководитель
к.ф.-м.н., доцент _____ А.Д. Панферов

Зав. кафедрой
к.ф.-м.н., доцент _____ Л.Б. Тяпаев

Саратов 2018

Введение. В настоящее время мировая экономика переживает этап формирования нового технологического уклада, в котором цифровые технологии, данные и информационные технологии играют очень важную роль. Если в двадцатом веке развитие опиралось на транспортные магистрали, трубопроводы и сети распределения электроэнергии, то сегодня приоритет принадлежит телекоммуникационным магистралям и сетям, обеспечивающим доступ к глобальной информационной сети Интернет любому человеку, в любое время и в любом месте.

Переход к использованию сети Интернет в качестве основного средства обмена личной, персональной, производственной и финансовой информацией поставили проблему её защиты от несанкционированного доступа. Острота этой проблемы определяет актуальность моей работы, целью которой является исследование современных средств защиты информации при её передаче в глобальной сети, особенностей сетевой инфраструктуры распределительных сетей в Республике Ирак и формулирование практических рецептов по обеспечению безопасности для пользователей услугами сети Интернет.

В Ираке в связи со сложностями политического процесса сетевая инфраструктура находится только в стадии развития и не может на должном уровне обеспечить потребности населения в информационных услугах. Поиску путей решения этой проблемы в условиях ограниченных экономических возможностей и высоких рисков безопасности посвящена моя выпускная квалификационная работа.

Основное содержание работы. Глобальная сеть внесла серьёзные изменения не только в способы получения информации, но и в формы и способы реализации многих других потребностей современного человека.

Через сеть реализуется межличностное общение. Это может быть переписка по электронной почте, обмен мгновенными текстовыми сообщениями, аудио диалог или полноценное видео общение. В таком общении мы раскрываем свои личные пристрастия и приоритеты, делимся

планами и прогнозами. В таком общении круг обсуждаемых тем и вопросов, уровень откровенности, количество раскрываемой информации и её достоверность по умолчанию определяются каждым из участников исходя из своих собственных интересов и уровня отношений с собеседником.

Все чаще через сеть мы выполняем большую или меньшую часть своих трудовых функций и обязанностей. В этом случае информационный обмен содержит корпоративную информацию в соответствии с вашими полномочиями и обязанности.

Если вы работаете в государственном учреждении, то уровень важности и ценности информации в таком обмене может иметь уже совсем другой уровень важности и ценности.

Мы постепенно привыкаем покупать в интернет магазинах. Диапазон таких покупок охватывает уже практически весь спектр товаров. От предметов первой необходимости, билетов в театры, до достаточно дорогостоящих услуг транспортных компаний и туроператоров. Мы переводим в сеть свои финансовые операции. Оплачиваем коммунальные услуги, берем и погашаем кредиты, распоряжаемся своими финансовыми активами. В этих случаях мы доверяем сети свою персональную и финансовую информацию.

При этом в большинстве случаев не принимается во внимание, что в этих диалогах может быть гораздо больше участников. Находясь наедине с компьютером или любым другим коммуникационным устройством у себя дома или в кабинете на работе легко забыть, что потоки данных преодолевают сотни и тысячи километров. Они проходят через сетевые устройства операторов сетей (и мы совершенно не имеем представления, сколько таких промежуточных устройств и кто их контролирует и администрирует).

Потоки данных в публичных сетях находятся под контролем государства. Если маршрут передачи ваших данных трансграничен, то интерес к ним могут проявить службы разных государств по совершенно разным причинам.

Доступ к глобальной сети свободен и сотни миллионов людей

пользуются её возможностями. При этом для некоторых из них этот интерес может быть корыстным и при этом вполне профессиональным, а предметом этого интереса служат чужие данные. Точнее те из них, обладание которыми может быть монетизировано.

В обычной жизни вне сети люди давно выработали правила обращения с данными и предметами, могущими быть предметом корыстного интереса. Дома мы запираем входную дверь и занавешиваем окна, запираем автомобиль и используем системы охраны различного типа. Для хранения документов, денег и ценных предметов используем сейфы. Интернет новая непривычная среда обитания. Главная проблема адаптации для её правильного использования - неочевидность её прозрачности и открытости.

С точки зрения информационной безопасности проблема заключается в том, что базовые принципы используемых сетью Интернет технологий разрабатывались для сетей с административно регламентируемым доступом, а затем адаптировались к открытым сетям в предположении, что передаваемая информация может рассматриваться как общественное достояние (например, научные данные). Поэтому они просто не имели механизмов для защиты от квалифицированного корыстного интереса.

С появлением в открытых сетях персональной, коммерческой и другой информации ограниченного доступа пришлось разрабатывать дополнительные протоколы и правила для её защиты. Это сложный и эволюционный процесс. В нем нет и не может быть одного общего для всех решения и окончательной победы. Как обычно, развитие средств защиты сопровождается совершенствованием оружия нападения.

Но можно уверенно констатировать, что прозрачного, открытого Интернета уже нет и никогда не будет. Предоставление любых коммерческих сервисов требует гарантированно высокого уровня защиты интересов клиента.

Знание современных протоколов защиты данных и умения применять их является обязательным требованием к специалисту, занимающемуся

эксплуатацией сетей и обеспечением предоставления услуг конечным пользователям. Необходимо уметь правильно объяснить риски использования сети Интернет, обеспечить клиента средствами защиты и предоставить понятные инструкции для их использования.

Проблема защиты данных в сетях общего пользования стала актуальной с формированием глобальной сетевой инфраструктуры Интернета и его превращением в инструмент ведения бизнеса, вплоть до осуществления финансовых операций. Массовое подключение к сети персональных пользователей привело к дополнительному резкому росту трафика и появлению в нем данных не только с корпоративной информацией разной степени конфиденциальности, но и персональных данных. Это спровоцировало еще в первой половине 90-х годов прошлого века два серьёзных кризиса: исчерпание адресных ресурсов исходной версии протокола IPv4 и проблему полной открытости данных в стеке TCP/IP.

Для решения этих проблем была намечена и реализована программа действий, которая рассматривалась как разработка новой версии протокола IPv6. К предложенным радикальным изменениям в системе адресации индустрия оказалась по ряду причин не готова и глобальная сеть еще примерно пятнадцать лет использовала усовершенствованную версию адресного пространства IPv4. А вот разработанный в рамках этой программы механизм защиты данных, известный как протокол IPsec, был успешно адаптирован для работы с использованием уже имевшейся базовой функциональности IPv4 и отлично зарекомендовал себя.

Замечательное преимущество этого инструмента - локализация всей функциональности в рамках сетевого уровня модели OSI. Он обеспечивает безопасное использование преимуществ сетевой инфраструктуры совершенно прозрачно (незаметно) не только для приложений, но и для сетевых протоколов верхних уровней.

IPsec — это структура открытых стандартов, независимая от алгоритмов.

Он обеспечивает конфиденциальность и целостность данных, а также аутентификацию источника. IPsec действует как протокол сетевого уровня, защищая пакеты IP и проверяя их подлинность. Для обозначения таких технологий может использоваться термин VPN (Virtual Private Network)-виртуальная частная сеть. Создавать виртуальные сетевые соединения и целые наложенные сети с различными уровнями защищенности поверх существующих сетей можно различными способами. IPsec один из наиболее часто встречающихся вариантов.

Первые документы, регламентирующие IPsec, были приняты в 1998-99 годах (RFC-2401-02, -2406, -2408 и -2709) [1,2]. Существуют версии IPsec для IPv4 и IPv6.

IPsec описывает способ обмена сообщениями для защиты сеансов связи на основе применения существующих алгоритмов [3]. Двумя основными элементами IPsec являются:

- Аутентифицирующий заголовок (Authentication Header, AH) - специальный протокол, применяемый в тех случаях, когда обеспечение конфиденциальности не требуется или запрещено. Он обеспечивает аутентификацию и целостность данных для пакетов IP, передаваемых между двумя системами. Однако AH не обеспечивает конфиденциальность (шифрования) данных в пакетах. Весь текст передаётся в открытом виде (без шифрования).
- Протокол шифрования полезной нагрузки (Encapsulating Security Payload, ESP) обеспечивает конфиденциальность и аутентификацию путем шифрования пакета IP. В процессе шифрования скрываются данные и идентификаторы источника и назначения. В ESP проверяется подлинность внутреннего пакета IP и заголовка ESP. Аутентификация обеспечивает проверку подлинности источника данных и целостность данных.

Альтернативой IPsec при работе в современной глобальной сети является протокол TLS, являющийся результатом развития протокола, появившегося с

именем SSL. Происхождение этих протоколов имеет те же причины - необходимость обеспечения безопасности в глобальной сети. И первая версия протокола SSL появилась в 1996 году, когда велась активная разработка IPsec. Но SSL был разработан частной компанией Netscape и его работа организована совершенно по другому с точки зрения модели OSI. Об этом говорит и само название Secure Sockets Layer (SSL) - слой (дополнительный) защиты сокетов [4].

С точки зрения OSI протокол размещается между двумя уровнями: протоколами, которые использует программа-клиент (HTTP, FTP, IMAP, LDAP, Telnet и т.д.) и транспортными протоколами TCP/IP. Создавая дополнительный барьер между ними, он работает с данными прикладных протоколов стека TCP/IP и передает их данные на транспортный уровень в уже защищенном виде. При этом SSL может поддерживать много разных протоколов прикладного уровня, используемых программами-клиентами.

Работу протокол SSL можно условно разделить на два уровня. Первый уровень – слой протокола подтверждения подключения (Handshake Protocol Layer). Он включает три субпротокола с различной функциональностью: протокол подтверждения подключения (Handshake Protocol), протокол изменения параметров шифра (Change Cipher Spec Protocol) и протокол предупреждений (Alert protocol). На втором уровне работает протокол записи.

Протокол подтверждения подключения используется для согласования данных сессии между клиентом и сервером. В данные сессии входят:

* идентификационный номер сессии;
* сертификаты каждой из сторон;
* алгоритм шифрования и его параметры;
* алгоритм сжатия;
* ключ сессии для симметричного шифрования

Протокол изменения параметров шифрования используется для изменения данных ключа сессии (keyingmaterial), который используется для

шифрования данных между клиентом и сервером. Протокол изменения параметров шифрования определяет формат и содержание сообщения, которым сервер уведомляет об изменении набора ключей.

Протокол предупредительных сообщений информирует стороны об изменение статуса или о возможной ошибке. Существует множество предупредительных сообщений, которыми стороны обмениваются как при нормальном функционировании, так и при возникновении ошибок. Как правило, предупреждения отсылаются тогда, когда подключение закрыто или получено неправильное сообщение, сообщение невозможно расшифровать или пользователь отменяет операцию.

В отличии от SSL, протокол TLS разрабатывался сообществом интернета сразу как универсальное средство, умеющее обслуживать любые протоколы прикладного уровня: электронной почты, обмена текстовыми сообщениями, аудио и видео телефонии.

Протокол за почти два десятилетия своего существования постоянно развивался. В него вводились новые механизмы для улучшения параметров защиты передаваемых данных, увеличения скорости работы и улучшения удобства использования.

Доступ к глобальной сети Интернет рассматривается в современном обществе как одно из основных прав человека, позволяющее реализовать для него свободный доступ к информации, социокультурное развитие и вовлеченность в процедуры управления развитием общества.

Для населения стран с развитой экономикой доступность интернета предполагается естественным элементом среды обитания. Но в Республике Ирак (РИ) пока еще предстоит много сделать для обеспечения всеобщего доступа к сетевой инфраструктуре. В решении этой задачи важную роль играет правительство. В соответствии с национальной политикой в области развития средств связи государство обеспечивает благоприятную и конкурентную среду

для необходимых инвестиций в инфраструктуру информационно-коммуникационных технологий и для развития новых услуг и сервисов.

В РИ развивается инфраструктура широкополосных сетей, спутниковых систем и других систем, чтобы помочь обеспечить потребности граждан в информационно-коммуникационных технологиях. Тем не менее, до настоящего времени коллективные сервисы доступа пользуются спросом. Поэтому наиболее простой способ выйти в глобальную сеть – воспользоваться услугами интернет-кафе. Час подключения тарифицируется в размере 1.0 – 1.5$, скорость соединения в большинстве кафе - от 256 кбит/с. Основным их контингентом является местная молодежь, играющая в компьютерные игры, либо общающаяся с родственниками и друзьями через социальные сети или с использованием он-лайн сервисов.

Магистральная телекоммуникационная инфраструктура Ирака сильно пострадала во время войны 2003 года. Официально количество государственных линий связи в настоящее время превысило довоенный уровень, но на практике почти все они используются госструктурами и контингентом иностранных войск. Услуги, предоставляемые гражданским лицам функционируют нестабильно, особенно их междугородный сегмент. Остаётся высокой и цена интернет-услуг для населения.

Доступные онлайн сервисы медленно работают при загрузке файлов и не обеспечивают необходимое качество для речевого и видео общения. Компании, занимающиеся предоставление услуг для выхода в Интернет физическим лицам, работают на рынке РИ с 2006 года. С этого времени можно отсчитывать эру массового доступа к сети Интернет. В 2011 году число пользователей сети Интернет в РИ превысило полтора миллиона человек. Но и сегодня остается большое количество иракцев, которые не пользуются Интернетом постоянно.

В Ираке на достаточно большой территории проживает менее сорока миллионов жителей. Поэтому для большинства поселений характерна малоэтажная жилая застройка с преобладанием двухэтажных строений. В этих

условиях с учетом невысокой платежеспособности жителей прокладка оптоволоконных кабелей к отдельным зданиям не рентабельно. Организация глубоких оптических вводов в районы жилой застройки с раздачей трафика через проводной Ethernet тоже неэффективна.

В таких условиях представляется целесообразным использование беспроводных технологий. На пользовательском уровне эффективно работают обычные Wi-Fi роутеры, обслуживающие одно жилое строение с одним собственником. При необходимости таким пользователям предоставляется техническая поддержка. Местная распределительная система строится на беспроводных технологиях средней дальности и состоит из центрального узла локального провайдера с антенной с круговой диаграммой направленности (360°) и приёмо-передатчиков абонентов, оснащаемых компактными NanoStatios (если расстояние небольшое, в ближней зоне) или направленными компактными параболическими антеннами в дальней зоне.

В работе представлена линейка оборудования фирмы Ubiquiti Networks, позволяющая полностью реализовать беспроводную систему распределенного доступа. Приведены примеры настройки этого оборудования для различных топологий сетей доступа. Оборудование хорошо зарекомендовало себя в сложных климатических условиях Ирака.

В условиях активного использования беспроводных технологий вопросы безопасности особенно актуальны. Сами базовые принципы работы таких сетей предоставляют злоумышленникам достаточно большой набор возможностей для попыток их взлома. Хотя WPA2 обеспечивает относительно высокий уровень безопасности, при наличии ресурсов и желания он не может быть полной гарантией безопасности.

Другие угрозы тоже должны приниматься во внимание.

В таких условиях предпочтительным выбором является использование VPN сервисов. Такой сервис можно организовать самостоятельно, но для массового не очень квалифицированного пользователя, предпочтительны

коммерческие платформы. Они не дороги и обеспечивают очень высокий гарантированный уровень защиты. Для их настройки предоставляется понятный и удобный интерфейс.

Конечно, использование VPN приводит к дополнительным издержкам. Возрастает нагрузка на вашу систему, поскольку ей приходится выполнять шифрование и дешифрование всего потока данных. Растет объём трафика. Это неизбежное неудобство, поскольку объём служебного трафика в защищенных протоколах гораздо выше. Наконец, время отклика сетевых ресурсов увеличивается. Последнее обстоятельство определяется тем, что теперь путь ваших данных всегда лежит через обслуживающий вас сервис. Кроме того, этот сервер выполняет их шифрование/дешифрование.

В результате проведенного анализа было установлено, что лучшей услугой VPN сейчас является сервис ExpressVPN. Это лучший универсальный вариант для скорости, конфиденциальности и разблокирования веб-сайтов. Ближайшим конкурентом является IPVanish, который тоже является очень надежным VPN с отличными характеристиками. Можно дополнительно отметить его умение оптимально работать с трафиком торрентов. Третий VPN, который необходимо отметить, - VyprVPN. Отличительной чертой последнего является очень высокая скорость обработки данных.

Практические рекомендации по установке и настройке клиентской части таких сервисов представлены.

Заключение. В представленной работе проанализированы проблемы обеспечения безопасности данных в публичных сетях. Рассмотрены особенности построения публичных сетей в Республике Ирак и их специфика.

В настоящее время передача персональных, медицинских, финансовых, корпоративных и других типов данных через глобальную сеть Интернет является обязательным условием функционирования многих социальных и коммерческих сервисов. Но это возможно только при гарантированном обеспечении их защиты. Способы такой защиты, их возможности, надежность,

особенности, варианты и механизмы реализации были подробно изучены.

Выработаны и представлены конкретные рекомендации по развертывании сетевой инфраструктуры в условиях жилого сектора низкой этажности на базе беспроводных технологий. Особое внимание уделено базовым возможностям этих технологий по защите передаваемой информации.

В качестве основного универсального средства обеспечения безопасности данных, работающего в сетях любого уровня, как на территории Ирака, так и за его пределами, предложено использовать VPN сервисы. Проведен анализ и сопоставление функциональности таких сервисов. Представлены подробные рекомендации по установке клиента такого сервиса.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1 IETF Documents [Электронный ресурс]. — URL: https://tools.ietf.org/html/ (Дата обращения 17.05.2018).

2 Коптев Д.С., Шевцов А.Н., Щитов А.Н., Наука и современность, 3(9), 133-142 (2016).

3 Семенов Ю.А., Алгоритмы телекоммуникационных сетей, Интернет-Университет Информационных Технологий: Москва, 512 с. (2007).

4 Overview of SSL/TLS Encryption [Электронный ресурс]. — URL: https://web.archive.org/web/20141202095453/https://technet.microsoft.com/en-us/library/cc781476(v=ws.10).aspx (Дата обращения 20.05.2018).

5 The transport layer security [Электронный ресурс]. — URL: https://tools.ietf.org/html/rfc5246#ref-TLS1.1 (Дата обращения 25.04.2018).

6 “Rocket5ac Lite” [Электронный ресурс]. — URL: https://www.ubnt.com/airmax/rocket-ac/ (Дата обращения 17.03.2018).

7 “Sector AM-V5G-Ti” [Электронный ресурс]. — URL: https://www.ubnt.com/airmax/airmax-ac-sector-antenna/ (Дата обращения 27.03.2018).

8 “NanoStation AC (5AC)” [Электронный ресурс]. — URL: https://www.ubnt.com/search/?q=NanoStation+AC+ (Дата обращения 9.04.2018).

9 “СРАВНЕНИЕ ЛУЧШИХ УСЛУГ VPN” [Электронный ресурс]. — URL: https://www.techradar.com/vpn/best-vpn (Дата обращения 6.05.2018).

10 “ExpressVPN” [Электронный ресурс]. — URL: https://expressvpn.com (Дата обращения 16.05.2018).