Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Лемешко К.Г., Бочалова И.О. Способы защиты информации в сети. шифрование данных. Анализ алгоритмов шифрования данных в сетях // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2017. – № 06 (июнь). – АРТ 224-эл. – 0,4 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.55

Лемешко Клавдия Геннадьевна,

Бочалова Ирина Олеговна

студентки 2 курс, факультет «Информатика и вычислительная техника»

Научный руководитель: Барашко Е.Н., старший преподаватель

Донской государственный технический университет

г. Ростов-на-Дону, Россия,

Email: lemeshcko.klavdia@yandex.ru

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ. ШИФРОВАНИЕ ДАННЫХ. АНАЛИЗ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ В СЕТИ

Аннотация: В статье рассматриваются современные виды шифрования в сети, способы защиты информации, анализ алгоритмов.

Ключевые слова: шифрование, алгоритмы шифрования, защита информации, информация, криптография, симметричное шифрования, ассиметричное шифрование, google, telegram.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Lemeshko Klavdiya Gennadievna,

Bochalova Irina Olegovna

students of the bachelor 2 course, faculty "computer science"

Supervisor: Barashko E. N., senior lecturer

Don State Technical University

Rostov-on-Don, Russian Federation

Email: lemeshcko.klavdia@yandex.ru

WAYS OF INFORMATION PROTECTION IN THE NETWORK. DATA ENCRYPTION. ANALYSIS OF NETWORK DIGITAL ALGORITHMS IN THE NETWORK

Annotation: The article considers modern types of encryption in the network, methods of information protection, analysis of algorithms.

Keywords: encryption, encryption algorithms, information protection, information, cryptography, symmetric encryption, asymmetric encryption, google, telegram.

С развитием компьютерной техники и информационных технологий, которые все больше проникают во все сферы жизни современного общества, острее встает вопрос информационной безопасности. Без должного внимания к вопросам обеспечения безопасности, последствия перехода общества к новым технологиям могут быть катастрофическими для него и его граждан.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

– расширением сферы использования электронно-вычислительных машин (ЭВМ), многообразием и повсеместным распространением информационно управляющих систем, высокими темпами увеличения парка средств вычислительной техники (СВТ) и связи;

– повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;

– вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса;

– концентрацией больших объёмов информации различного назначения и принадлежности на электронных носителях;

– количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;

– отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг.

Под безопасностью подразумевается совокупность трех различных характеристик системы, обеспечивающей безопасность:

– аутентификация – процесс распознавания системой пользователя и предоставления ему доступа к некоторым своим возможностям;

– целостность – состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий. Например, в случае передачи данных под целостностью понимается идентичность отправленного и принятого;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

– секретность – предотвращение несанкционированного доступа к информации.

Сегодня очень многие фирмы используют открытый доступ в Internet в качестве основного способа доступа к своим базам данных для сотрудников. Большое количество операций выполняется так же в среде Internet. Это финансовые операции, заказ товаров и услуг, удаленная работа, передача важной информации и так далее. Такая деятельность требуют защиты повышенного уровня.

Для обеспечения секретности активно применяется *шифрование*, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа. Шифрование и программное удаление информации является ключевым и доступным большинству пользователей вариантом скрытия информации на носителях в случае экстренной необходимости.

В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм – это способ закодировать исходный текст, в результате чего получается зашифрованное послание, которое может быть интерпретировано только с помощью ключа. На сегодняшний день известны две основные схемы шифрования: *симметричное* шифрование и шифрование *с открытым ключом* (асимметричное).

При использовании *симметричного шифрования* отправитель и получатель имеют один секретный ключ на двоих, с помощью которого они могут зашифровать и расшифровать данные. Используемые ключи имеют небольшую длину, поэтому можно шифровать достаточно большие объемы данных, но симметричное шифрование обладает некоторыми недостатками. Во-первых, очень сложно найти безопасный способ передачи ключа отправителю и получателю. Во-вторых, для каждого из двух сторон

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

необходимо хранить отдельный секретный ключ. В-третьих, невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.

При *ассиметричном способе* (шифрование с открытым ключом) для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи другого – расшифровывается. Благодаря этому, требуемого уровня безопасности можно добиться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя (закрытый, личный ключ). При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга. Недостатком асимметричного шифрования можно считать использование более длинных ключей, чем при симметричном шифровании. Такие ключи из-за своих размеров сильно влияют на вычислительные ресурсы, требуемые для организации процесса шифрования, обеспечивая при этом подобный уровень безопасности.

В асимметричных системах необходимо применять длинные ключи (512 битов и больше). Длинный ключ резко увеличивает время шифрования. Кроме того, генерация ключей весьма длительна. Зато распределять ключи можно по незащищенным каналам.

В симметричных алгоритмах используют более короткие ключи, т. е. шифрование происходит быстрее. Но в таких системах сложно распределение ключей.

Поэтому при проектировании защищенной системы часто применяют и симметричные, и асимметричные алгоритмы. Так как система с открытыми ключами позволяет распределять ключи и в симметричных

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

системах, можно объединить в системе передачи защищенной информации асимметричный и симметричный алгоритмы шифрования. С помощью первого рассылать ключи, вторым же - собственно шифровать передаваемую информацию Обмен информацией можно осуществлять следующим образом:

– получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным;

– отправитель, используя открытый ключ получателя, зашифровывает сеансовый ключ, который пересылается получателю по незащищенному каналу;

– получатель получает сеансовый ключ и расшифровывает его, используя свой секретный ключ;

– отправитель зашифровывает сообщение сеансовым ключом и пересылает получателю;

– получатель получает сообщение и расшифровывает его.

Google популярный интернет-поисковик начнет назначать более высокий приоритет на веб-сайты, которые используют своего рода шифрования, известный как HTTPS, это значительный шаг в направлении повышения безопасности и конфиденциальности в Интернете.

Google потратил десятки миллионов долларов, чтобы усилить свои онлайновые услуги в последние годы. Это также толкаемых для более широкого использования шифрования, всей отрасли, как защититься от технически подкованных преступников и, после прошлогоднего откровения о шпионаже спорным Агентства национальной безопасности, сократить слежка государственными органами. Поисковая система Google используется примерно две трети всех пользователей Интернета, и тщательно исследовали критиками и регулирующими органами каких-либо

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

признаков, что он злоупотребляет, что доминирование путем обработки участков несправедливо. Но Google использует свои алгоритмы в прошлом, чтобы держаться подальше от посетителей определенных сайтов, таких, как известно, заражен вредоносными программами.

Протокол HTTPS (HypertextTransferProtocolSecure) представляет собой расширение стандартного протокола HTTP. Его принципиальным отличием является поддержка шифрования данных. Защита передаваемой информации обеспечивается благодаря криптографическому протоколу SSL или TLS. Основная область применения HTTPS – облачные приложения, которые требуют повышенной защиты, например, платежные системы. Протокол HTTPS был разработан в компании Netscape Communications Corporation для возможности обеспечения аутентификации и защищенного соединения. В настоящее время HTTPS наряду с HTTP являются наиболее популярными протоколами в мире, их поддерживают все современные браузеры.

Снифферские атаки основаны на фальсификации либо прослушивании сетевого соединения, когда перехват происходит на пути переноса данных от компьютера к банку.

Использование HTTPS позволяет снизить вероятность снифферских атак, при которых хакер перехватывает пакеты для дальнейшего анализа их содержания, и атак вида man-in-the-middle, когда злоумышленник способен не просто перехватить данные, а удалить их часть или заменить ложной информацией. Максимальная степень защиты обеспечивается при применении шифрующих средств и проверке сертификатов сервера.

Для передачи данных по протоколу HTTPS используется 443-й порт, а не 80-й, как в стандартном HTTP. Чтобы работать с https-соединениями,

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

на сервер необходимо установить сертификат, состоящий из 2 частей – public и private.

Цифровой сертификат — это файл, который уникальным образом идентифицирует пользователей и серверы. Это своего рода электронный паспорт, который проводит аутентификацию сервера до того, как устанавливается сеанс SSL соединения.

Преимущества HTTPS для SEO. HTTPS вошел в жизнь SEO довольно давно. Еще в 2014 году Google рекомендовал всем сайтам перейти на защищенное соединение. Он сделал это сам и с подвиг другие сайты использовать более безопасное соединение. После этого начались дискуссии о необходимости использования зашифрованного соединения, целесообразности и выгоде от перехода на SSL. Осенью 2014 года Google включил HTTPS в алгоритм ранжирования сайтов и с этого момента HTTPS неотрывно связан с SEO и комплексным продвижением сайта.

В 2016 году уже не стоит вопрос о необходимости перехода на HTTPS, так как наличие SSL сертификата это «musthave» для каждого сайта или проекта. Не важно, банк вы или интернет-магазин, блог о рыбалке или сайт правительства – защита данных вашего сайта и персональных данных пользователей обязательное условие в современном интернете.

Также, совсем недавно Google объявил, что с января 2017 года будет отмечать сайты, использующие HTTP как небезопасные.

Недостатки HTTPS для SEO. Несмотря на наличие явных преимуществ, у многих владельцев сайтов может возникнуть ряд проблем в использовании SSL на своих сайтах:

– Цена вопроса. SSL сертификаты есть как бесплатные, так и платные. При этом цена может существенно различаться: от 1500 руб/год до 15000 руб/год. Все зависит от уровня сертификата и количества доменов.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

– Технические сложности. При переходе с HTTP на HTTPS меняется адрес всех страниц сайта.

– Посещаемость сайта снизиться. На первых порах, в течении недель или месяца после переезда, на сайте будет наблюдаться спад трафика из органики. Это связано в первую очередь с обработкой поисковыми системами сайта на с https://. После того, как сайт с новым протоколом обработает Google, позиции восстановятся и даже вырастут.

По данным компании ***Mozilla***, объем зашифрованного трафика в интернете наконец-то превысил объем незашифрованного. Увидеть в адресной строке слева пиктограмму в виде зелёного замочка можно гораздо чаще, чем раньше. Подобная пиктограмма означает, что подключение осуществляется по защищенному протоколу HTTPS, а не по HTTP, предающему данные в открытом виде. По состоянию на 29 января 2017 года на долю HTTPS-трафика пришлось 50,01764%. Отставание HTTP не такое уж большое, но в принципе его можно считать «стратегическим рубежом», который преодолел HTTPS.

Выводы Mozilla сделаны на основании средних показателей объема зашифрованного и незашифрованного трафика за две недели, и в ближайшие дни они еще могут колебаться. Тем не менее, сам факт того, что зашифрованному трафику удалось превысить по количеству незашифрованный, уже является значительным событием. «Значение этого переломного момента трудно переоценить», – цитирует издание Wired эксперта организации NewAmerica Росса Шульмана (RossSchulman).

Telegram – бесплатный кроссплатформенный мессенджер для смартфонов и других устройств, позволяющий обмениваться текстовыми сообщениями и медиафайлами различных форматов. Используются проприетарная серверная часть с закрытым кодом, работающая на

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

мощностях нескольких компаний США и Германии, финансируемых Павлом Дуровым в объёме порядка 12 млн долларов США ежегодно, и несколько клиентов с открытым исходным кодом, в том числе под GNU GPL.

Учётные записи пользователей привязываются к телефонным номерам, что является одним из самых существенных аргументов критиков Telegram, поскольку это не обеспечивает полной анонимности при общении. При регистрации в сервисе и последующих авторизациях новых устройств, производится проверка телефонного номера через отправку SMS-сообщения с кодом (на некоторых ОС – перехватывается приложением) или телефонный вызов.

Количество активных пользователей сервиса на февраль 2016 года составляло более 100 млн человек, а количество ежедневно пересылаемых сообщений достигло 10 миллиардов на август 2015.

Основное достоинство ***Telegram*** сетевая защищенность переписки.

Подробнее о плюсах технологии ***Telegram***:

– Защита от несанкционированного чтения осуществляется благодаря применению протокола связи MTProto.

– Наличие опции переписки в «секретном чате» SecretChat. Благодаря ней вы можете общаться при помощи зашифрованных сообщений.

– Наличие таймера для автоуничтожения сообщений спустя заданное время (например, 1 час, а не через максимум всего 10 секунд, как в Viber).

– Возможность передачи файлов большого размера (до 1 Гб).

– Высочайшая скорость работы, в т.ч. доставки ваших файлов адресату. Нет задержек, характерных другим мессенджерам.

– Синхронизация между пользователями.

Минусы технологии ***Telegram***:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

– Несмотря на российское авторство, изначально Telegram не поддерживает в меню интерфейса русский язык. Многих это расстраивает. Могу лишь сказать следующее: Программа интуитивно понятна и на английском языке, как вариант вы получаете возможность его подучить. Общаться же, разумеется, можно и по-русски Русификация делается буквально за полминуты путем запроса языкового пакета роботу и его установки по нехитрой инструкции:

– Другой недостаток отсутствие возможности голосовых звонков. В отличие от конкурентов, где они давно имеются.

Шифрование Телеграмм на основе ***MTProto.***

Протокол MTProto использует два слоя шифрования – сервер-сервер и клиент-сервер. Он работает на основе следующих алгоритмов: Алгоритм показывает, как используется шифрование Телеграмм на основе MTProto

– AES – симметричный 256-битный алгоритм, принятый правительством США в качестве стандарта.

– RSA – криптографический алгоритм, в основе которого лежит вычислительная сложность задачи факторизации крупных целых чисел.

– Метод Диффи-Хеллмана – позволяет получить двум и более собеседникам секретный ключ по незащищенному от прослушивания, однако защищенному от подмены каналу связи.

– SHA-1, MD5 – хеш-алгоритмы, используемые во многих криптографических протоколах и приложениях для безопасного хеширования.

Создатели мессенджера заявляют о гарантии безопасности в отношении передачи зашифрованных данных. Для подтверждения своих слов Павел Дуров периодически организовывает конкурсы, в которых участникам предлагается расшифровать переписку двух собеседников.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Призовой форд составляет 200 тыс. долларов, однако до настоящего времени ни один хакер не смог прочитать зашифрованные сообщения.

Google и Telegram доминирует на поисковом рынке – на сервис компаний приходится около 90% всех мировых запросов, и бизнес многих компаний полностью зависит от места сайта в результатах поиска. Google и Telegram постоянно совершенствуют алгоритмы шифрования данных. Конкуренция с Telegram заставила многие компании пересмотреть свою политику безопасности. В связи с этим, был введен принцип оконечного шифрования, который с 2016 года стал использоваться по умолчанию. Его суть заключается в хранении ключей, необходимых для расшифровки сообщений, только на устройстве пользователя. Таким образом, чтобы получить доступ к информации, необходимо обладать физическим доступом к устройству.

Список использованной литературы:

1. Веб-сайт:http://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi
2. Веб-сайт:http://www.mobile-networks.ru/ articles/201601/myisli_o_telegram_plyusyi_i_minusyi.html
3. https://www.google.com/transparencyreport/https/?hl=ru
4. Лапонина, О.Р.Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / О. Р. Лапонина; Лапонина О. Р. - 2016. - 242 с.

Дата поступления в редакцию: 10.06.2017 г.
Опубликовано: 13.06.2017 г.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Для заметок