МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования **«Крымский федеральный университет имени В. И. Вернадского»**

Таврическая академия (структурное подразделение)

Факультет математики и информатики

Кафедра прикладной математики

Консманов Алексей Витальевич

Сохранение тайны связи в условиях новых цифровых угроз

Курсовая работа

Обучающегося	**3 курса**
Направления подготовки	**01.03.04**
Форма обучения	**очная**

Научный руководитель — старший преподаватель кафедры прикладной математики В. А. Лушников

Симферополь 2018

Оглавление

Введение

В настоящее время на рынке информационных технологий представлено множество средств защиты личных и корпоративных данных. Однако, средства проведения информационных атак развиваются быстрее, чем имеющиеся средства защиты, таким образом создавая "черный"рынок с вредоносным программным обеспечением и множеством разнообразных математических и социальных алгоритмов проведения атак.

Анализ инцидентов информационной безопасности, проведенный в конце 2016 года международной компанией «Positive Technologies» показал, что в 2017 ожидается на 30% больше инцидентов по информационной безопасности в финансовой сфере и появление новых, более убедительных средств социальной инженерии.

Также, исследования «Angara Technologies Group» показывают, что многие сотрудники как частного, так и государственного сектора слабо информированы и обучены правилам обращения с данными внутри организаций, что приводит к растущему числу утечек организационных и личных данных по аналоговым (физическим) и цифровым (информационным) каналам. Кроме очевидного, сложно измеримого вреда деловой репутации, отмечаются более понятные негативные последствия утечек — отмена сделок, компенсация ущерба третьим лицам, затраты на судопроизводство.

Исходя из данных результатов исследований и прогнозов, можно сделать вывод о необходимости развития социальных и алгоритмических методов защиты личных данных, в том числе защиты тайн переписки и связи.

Актуальность работы связана с возросшим числом новых угроз в области защиты личных данных, участившимися атаками частных лиц, группировок и специальных ведомств иностранных государств против частных лиц с целью получения частной информации, анализа полученных личных данных и использования для шантажа атакуемых лиц, продажи или другого выгодного обмена, а также в иных противозаконных целях. Данная курсовая работа может быть актуальна в рамках изучения дисциплин связанных с защитой данных и программирования

на факультетах математики и информатики, практическая часть работы представляющая собой несколько криптографических алгоритмов вместе с их реализацией может быть использована для изучения современных промышленных языков программирования (C, C++, C#). Полученная в результате анализа угроз информация применима для защиты данных, особенно переписки, частных лиц в общественных и частных сетях. Также, разработанные рекомендации и реализации алгоритмов могут быть применены частными лицами и предприятиями, государственными структурами, в том числе на коммерческой основе.

Целью данной работы является анализ новых цифровых угроз, возникших в последнее десятилетие в связи с бурным развитием информационных технологий, за которым не последовал соразмерный рост знаний пользователей цифровых систем, используемые кибер-преступниками методы анализа и атаки на частные данные, правовой аспект защиты личной переписки и тайны связи, способы борьбы с угрозами в рамках существующего программного обеспечения, сравнительный анализ существующих продуктов, разработка и реализация собственных алгоритмов для сохранения тайны связи.

В качестве **объектов исследования** выбраны цифровые данные частных лиц в приватных и организационных сетях, в первую очередь сама переписка и сведения об абонентах, то есть участниках переписки.

Предмет исследования: изучение методов атак на частные данные, причины утечек этих данных, цели, преследуемые злоумышленниками при проведении атак на частные данные и переписку. Предметы выбраны с целью создания математических и социальных алгоритмов защиты частных данных и переписки.

1 Понятия «тайна связи» и «личная переписка» в правом и информационном аспектах

1.1 Понятия в правовом аспекте

Так как все пользователь информационных систем являются в первую очередь гражданами правовых государств и объектами и субъектами права, рассмотрение основных понятий начнём с правого аспекта вопроса.

Согласно статье 63 федерального закона «О связи»: «На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.» Федеральный закон "Об информации, информационных технологиях и о защите информации"от 27.07.2006 №149 определяет набор правовых, организационных и технических мер, целью которых является защита информации от неправомерного доступа, модификации, блокирования, копирования и распространения. Также вводится ответственность за правонарушения в сфере информационных технологий и защиты информации. Устанавливается понятие **информации** как сведений (данных, сообщений) независимо от их формы представления, **информационно-телекоммуникационной сети** как "технологической системы, предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники ".

Исходя из данных законов, в дальнейшем под «**тайной связи**» будет подразумеваться совокупность тайны переписки, телефонных разговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи, сетям почтовой связи и информационно-телекоммуникационным сетям. Из определения последней очевидно, что к такой сети можно отнести сеть «Интернет»

Понятие **«личная переписка»** в данной работе подразумевает информацию личного характера, не составляющую коммерческую, госу-

дарственную или другую тайну, передаваемую любым способом, который используется в «тайне связи » и «тайне связи в Интернете».

Подобные законы существуют в большинстве развитых стран. Например, четвертая поправка к Конституции США гласит : «Право народа на охрану личности, жилища, бумаг и имущества от необоснованных обысков и арестов не должно нарушаться. Ни один ордер не должен выдаваться иначе, как при наличии достаточного основания, подтвержденного присягой или торжественным заявлением; при этом ордер должен содержать подробное описание места, подлежащего обыску, лиц или предметов, подлежащих аресту».В ЕС с 2016 года на смену Data Protection Directive(директива 95/46/EC) пришел General Data Protection Regulation, GDPR (Общеевропейский регламент о персональных данных), обязательный для всех организаций на территории ЕС, осуществляющих обработку персональных данных, в том числе, связанных с тайной связи и переписки. Подл действия регламента попадают данные, позволяющие непосредственно или косвенно определить личность человека, к которому эти данные относятся: IP-адрес, cookie ID, банковские данные, персональная информация и переписка, имя,адрес электронной почты, проживания или фактического нахождения. Физические лица получат право на забвение, на исправление, доступа – знать, какая информация хранится и как обрабатывается, на ограниченную обработку – блокировать или запрещать обработку , перенос данных и возражение – аналогично праву на блокировку применимо к маркетингу и научным статистическим исследованиям.

Введём понятие «**тайны связи в Интернете**», дополнив исходное понятие и изменив область приложения. Под «тайной связи в Интернете» в дальнейшем будет подразумеваться совокупность правовых норм, алгоритмов и методов сохранения секретности и непубличности (известность и доступность только абонентам) содержимого самого сообщения, информации о его абонентах (получателе или получателях и отправителе), условиях передачи сообщения (время, место отправки и получения, используемое при этом оборудование).

Нарушениями тайны связи не является :

- Прослушивание (в том числе и обыск) без ордера в случае проведе-

ния контрразведывательных операций. Однако подобное допустимо только при условии наличия достаточных оснований и обоснования того, почему в конкретном случае получение ордера не целесообразно. При этом правоохранительные органы могут искать лишь доказательства, подтверждающие факты действия разведывательных органов иностранных государств.

- Во многих странах заключённые и их вещи могут обыскиваться без каких-либо оснований в любое время, так-как подобное является частью режима лишения свободы, применённого к заключённому по решению суда. Аналогичное касается электронной и прочих видов связи.

- Контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи являются видами оперативно-разыскных мероприятий. Их проведение в Российской Федерации допустимо на основании судебного решения и при наличии информации о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации; о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно; о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно.

Применимо к особенностям организации общения и передачи данных в Интернете, под **«нарушением тайны связи»** будут подразумеваться следующие ситуации :

- Передача стороной, предоставляющей услуги связи, данных об абонентах связи, времени связи и прочих параметрах сообщений третьим лицам.

- Проведение атаки на любые физические компоненты коммуникационных сетей : ЭВМ пользователей или стороны, предоставляющей

услуги связи, сетевое оборудование, серверы; атаки типа «Man in the middle», выполняемые непосредственно на линиях связи.

- Использование правоохранительными органами прослушивающего оборудования без соответствующих санкций (ордера) суда или другие действия, выходящие за рамки полномочий правоохранительных органов, ведомств и силовых структур данного государства.

- Перехват сообщений на аналоговых носителях с целью их изучения и/или модификации с последующей передачей изначальному адресату; аналогичный перехват с целью изучения и уничтожения или перехват с целью уничтожения без изучения.

- Преступная халатность, повлекшая попадание частных данных в руки третьих лиц.

2 Понятие «цифровой угрозы» , новые цифровые угрозы

Дадим определение понятию « цифровая угроза » и рассмотрим их основные виды.

2.1 Определение

Цифровая угроза – совокупность условий и факторов, создающих опасность нарушения информационной безопасности в контексте нарушения тайны связи.«Цифровая угроза» является частным случаем *угрозы информационной безопасности* – угрозой конфиденциальности (неправомерный доступ к информации) и угрозой доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

Угрозы называются «**новыми**», так как их бурное развитие и рост числа инцидентов произошли в последние 10-15 лет и сами угрозы постоянно меняются, увеличивается их количество.

2.2 Основные виды угроз в частном секторе

Основными видами новых цифровых угроз являются утечки и перехваты сообщений, происходящие с помощью SpyWare (подмножество вирусов), целенаправленных атак на протоколы и средства связи,атак на криптографические протоколы, халатность отправителя, состоящая в использовании недоверенных сетей и средств. Рассмотрим каждый вид подробнее.

SpyWare. Вирус в классическом понимании представляет собой программы, целенаправленно создающие свои копии и передающие их по разным каналам связи на другие устройства , способные внедряться в код других программ, загрузочные секторы жёстких дисков. При этом основной функцией вируса является саморепликация и распространение, а модификация работы аппаратно-программных комплексов – всего лишь сопутствующая функция. SpyWare (сокр от Spy Software – «Шпионское программное обеспечение») представляет отдельный класс вредоносного ПО, лишенный репликативных свойств вируса. Основным назначением SpyWare является мониторинг, сохранение и передача злоумышленнику

данных о работе ПО, пользовательской активности и самом пользователе на заражённом устройстве. Установка таких программ происходит скрытно и не предполагает возможности пользователя следить за работой такой программы или её удаления. Для перехвата сообщений используются кейлоггеры(keyloggers), осуществляющие логирование всех нажатых клавиш, скрин-скраперы(screen scrapers), создающие снимки экрана через заданный интервал времени или по наступлению события, и обобщенные следящие программы, способные перехватывать содержимое почтовых программ и веб-страниц, открытых на заражённом устройстве, с помощью post-get запросов и автоматизированных средств взаимодействия с веб-браузером таких как Selenium.

К SpyWare не относятся программы, добровольно установленные пользователем и применяющиеся на совершенно законных основаниях для мониторинга состояния устройства, оказания удалённой технической поддержки,исследования защищённости компьютерных систем, желаемых пользователем персонализации и обновления компонентов ПО.

Рассмотрим отдельно самого распространённого представителя SpyWare – **кейлоггер** – программный или аппаратный комплекс, регистрирующий взаимодействие пользователя с устройствами ввода-вывода, в классическом случае – с клавиатурой и мышкой. Первые кейлоггеры появились в эпоху MS-DOS и представляли собой перехватчик прерывания int 16h.

Современные компьютеры, работающие в protected mode, не дают программисту доступ к таким низкоуровневым возможностям, поэтому теперь в основе современных кейлоггеров лежит использование **хуков** – технологии, позволяющей изменить стандартное поведение тех или иных компонентов информационной системы. Обычно для этого используются компоненты Win32API: WH_Keyboard, WH_JOURNALRECORD. Преимущество последнего заключается в отсутствии необходимости использования DLL, что упрощает распространения вируса через компьютерные сети. Недостатком использования хуков является легкая обнаружимость DLL с хуком, так как для перехвата нажатий DLL отображается в адресное пространство всех GUI-процессов.

Второй популярной методикой является циклический опрос состо-

яния клавиатуры с высокой скоростью. Преимуществом является меньшая заметность кейлоггера, однако присутствует значительный недостаток – необходимость очень частого опроса клавиатуры, примерно 10-20 опросов в секунду – современные ОС могут не выделить процессу с низким приоритетов столько ресурсов или не предоставлять доступ с такой частотой.

Третий способ является одним из наиболее эффективных и представляет собой кейлоггер уровня драйвера. В таком случае кейлоггер является частью драйвера, незаметен для большинства антивирусов, не может быть удален без потери функциональности клавиатуры. Также возможна реализация драйвера-фильтра, являющегося прослойкой между настоящим драйвером и ОС. Также к низкоуровневым кейлоггерам может быть отнесен руткит, перехватывающий обмен csrss.exe (Server Client Runtime Subsystem)

В последнее время на рынке гаджетов появились аппаратные клавиатурные устройства, имеющие сходный с программным кейлоггером функционал, представляющие собой USB-флешки, регистрирующие нажатия клавиш и записывающие их на собственную память. Такое устройство может автономно работать достаточно долго. Если предположить, что средний менеджер нажимает примерно 23000 клавиши в день(обозначим константой ApD), один символ занимает 1 килобайт памяти (обозначен переменной S) и взять емкость запоминающего устройства 16Gb (обозначим константой Mem), то памяти хватит на $\frac{Mem}{Apd*S} = \frac{16Gb}{23000*9{,}54*10^{-7}Gb}$ = 727 дней автономной работы.

Атаки на протоколы и средства связи

Большинство атак на протоколы связи основаны на принципе **«Человек в середине»** или «Атака посредника» («Man in the midle», MITM). В основе такой атаки лежит перехват сообщений на линии коммуникации между отправителем и абонементом. При этом возможны два метода атаки: пассивное прослушивание заключается в перехвате и анализе сообщений, если они зашифрованы, активная атака предполагает перехват, анализ сообщений, взлом криптографических алгоритмов, если такие используются, изменение содержимого сообщения и/или предотвращение передачи без разрушения канала связи.

Современные протоколы коммуникации используют различные криптографические протоколы, при этом шифрование происходит непосредственно на устройствах, то есть через коммуникационные сети передается уже зашифрованное сообщение, которое невозможно просто прочитать или модифицировать, не взломав ключ шифрования или не использовав другую уязвимость, поэтому будут рассмотрены именно активные методы атаки.

Пример атаки на алгоритмическом языке: Алиса хочет передать сообщение Бобу, Мэлори хочет перехватить и, возможно, изменить его так, чтобы Боб получил злонамеренно ошибочное сообщение:

1 Алиса отправляет сообщение Бобу, сообщение перехватывает Мэлори;

2 Мэлори пересылает сообщение Бобу, который не знает, что сообщение не от Алисы;

3 Боб посылает свой ключ;

4 Мэлори подменяет ключ Боба своим, затем пересылает сообщение Алисе;

5 Алиса принимает сообщение, шифрует свое сообщение ключом Мэлори, который считает ключом Боба и что только он сможет расшифровать его, отправляет сообщение Бобу;

6 Мэлори перехватывает сообщение, шифрованное ключом Мэлори (лже-Боба), модифицирует его, шифрует ключом Боба и отправляет Бобу;

7 Теперь Мэлори может модифицировать сообщения обеих сторон, даже если те решат изменить ключи.

Атаки типа MIT показывают важность точного подтверждения того, что обе стороны используют настоящие открытые ключи: у стороны A открытый ключ стороны B и у стороны B открытый ключ A. Если такое подтверждение не используется, то канал может быть атакован по принципу MIT.

Атаки на криптографические протоколы Криптографические протоколы в зависимости от сложности решают одну или несколько задач: шифрование/дешифрование, создание электронной цифровой подписи (ЭЦП, digital signature, DS), идентификация/аутентификация, аутентифицированного распределение ключей. Атаки на протоколы можно разделить на пассивные и активные: при пассивных атаках взломщик(криптоанали не участвует в протоколах, только следит за протоколом и пытается раздобыть ценную информацию на основе перехватываемого шифротекста; при активных атаках аналитик пытается изменить протокол к собственной выгоде и для этой цели активный взломщик может выдавать себя за другого человека, повторять или заменять сообщения, разрывать линию, модифицировать информацию. В целом, классификация атак на криптографические протоколы совпадает с классификацией атак на сетевые коммуникационные протоколы.

Рассмотрим самые широко известные атаки на криптографические протоколы:

Подмена. Метод атаки заключается в подмене одного контрагента переписки другим. Аналитик, выступая от имени одной стороны коммуникации, полностью имитирует её действия, получает сообщения определенного формата, необходимые для анализа шифротекста и подделки определенных шагов протокола.

Повторное навязывание сообщения (replay attack). Атака основана на повторной передаче ранее переданных в текущей или прошедших сессиях сообщений или частей сообщения. Например, повторная передача информации проведенного ранее протокола идентификации/аутентификации может привести к повторной успешной идентификации/аутентификации атакующего как настоящего контрагента общения. Такая атака также может быть использована в протоколах передачи ключей для навязывания ранее использованного сеансового ключа и известна как атака на основе новизны (freshness attack).

Параллельная атака (parallel-session attack). Аналитик открывает несколько параллельных сессий, при этом сообщения и полученные аналитиком данные из одного сеанса используются для анализа шифротекста и ключей другого сеанса.

Атака с использованием специально подобранных текстов. Атака на post-get запросы, при которой аналитик по определенному правилу подбирает запросы и их содержимое с целью анализа долговременного ключа собеседника.

Атака по известному сеансовому ключу (known-key attack). Заключается в получении долговременных ключей, новых сессионных ключей или установлении алгоритма, используемого для генерации новых ключей по известному использованному ранее сессионному ключу.

Использование уязвимостей алгоритма или ошибок реализации . В атаках такого типа аналитик ищет уязвимости, связанные с алгоритмом или ошибки реализации. Такая атака может давать самые долговременные и серьезные результаты, так как для успешного отражения контрагентам необходимо узнать о компрометации используемого алгоритма и внести исправления в алгоритм и его реализацию. Однако, такая атака является достаточно затруднительной для аналитика, так как требует реверс-инжиниринга алгоритма и его реализации, что может быть затруднительно в реальных коммуникационных сетях, где аналитику доступен только шифротекст и время отправки сообщения.

Перечисленные выше угрозы относятся к частному и корпоративному общению, при этом государство или несколько государств не являются стороной коммуникации или криптоаналитиком. Ниже рассмотрим теоретические ситуации и конкретные прецеденты, когда государство (под «государством» далее понимается совокупность судебной, законодательной и исполнительной властей конкретного государства) является криптоаналитиком или пособником аналитика по отношению к своим или иностранным гражданам.

2.3 Наблюдение и контроль за коммуникациями со стороны государства

Современные законотворческие инициативы ведущих стран Европы, Америки и Азии содержат в себе идею борьбы с терроризмом, опасность которого действительно невозможно не заметить, посредством массовой

перлюстрации (просмотр личной пересылаемой корреспонденции, совершаемый втайне от контрагентов) или явного анализа цифровой переписки.

Основной проблемой в контексте тайны связи является возможность недобросовестного использования полученных данных с целью шантажа или продажи, утечки из государственных информационных систем и хранилищ. Вторым большим опасением можно считать тот факт, что для доступа к переписке разработчики ПО оставляют backdoor'ы – дефект алгоритма, намеренно встраиваемый в него разработчиком и позволяющий получить несанкционированный доступ к данным, и если такой backdoor существует, то нет никаких гарантий, что доступ к нему не будет получен третьими лицами, что попадает под «нарушение тайны связи» из части 1 данной работы.

Рассмотрим такие ситуации на примерах крупнейших мировых государств:

Китай. КНР проводит политику массовой слежки за гражданами по всей территории страны. В рамках этой политики реализованы два масштабных проекта:

«Золотой щит» (Великий китайский фаервол). Представляет собой систему фильтрации содержимого интернета. Разрабатывался с 1998, введен в эксплуатацию повсеместно с 2003. Включает подсистемы управления безопасностью, информирования о правонарушениях, контроля входа и выхода, мониторинга и управления трафиком. Функции проекта: ограничения доступа к ряду иностранных сайтов, ограничение публикаций для китайских СМИ, перехват и хранение сообщений в мессенджерах.

Интернет-цензура. Включает в себя вышеописанный «Золотой щит» и комплекс мер, используемых правительством КНР для перехвата сообщений в мессенджерах и других средствах коммуникации, использующих защиту данных. Помимо использования стандартных приемов слежки, власти КНР используют социальные приемы. Так была создана социальная сеть «Sina Weibo» – собственный проект китайской компанией Sina Corp в 2009 году. Существует мнение, что Sina Corp предоставляет доступ к данным и переписке пользователей правительству КНР, при

этом сами пользователи считают, что их данные находятся под надёжной защитой владельцев платформы.

Параллельно с двумя вышеупомянутыми проектами в КНР в тестовом режиме работает система **«Система социального кредита»** – система постоянного анализа поведения граждан в Интернете и в повседневной жизни. При этом в качестве поощрения и наказания выступают разрешение на работу в госучреждениях, возможность получать соцобеспечение, повышенное внимание таможни, возможность покупки билетов на самолеты и поезда, право на обучение детей в частных дорогих школах.

США и ЕС. Несмотря на значительный уровень свободы слова и уважения к частной жизни, декларируемые Конституцией США, в государстве имеется широкая и мощная сеть компьютерного слежения и радиоэлектронной разведки. Задачи разведки и слежения возложены на АНБ, ФБР, ЦРУ, Министерство финансов, Министерство обороны, Министерство юстиции и Министерство внутренней безопасности США.

Рассмотрим подробнее основные программы слежения США и ЕС:

MAINWAY. База данных, содержащая метаданные о нескольких миллиардах телефонных звонков, совершенных через самые крупные коммуникационные компании США: AT&T, SBC, BellSouth, Verizon. Проект находится в ведении АНБ и имеет несколько дочерних: Stellar Wing – программа слежения за электронной активностью, в том числе электронной почтой, телефонными звонками, активностью в Интернете, имевшая место во времена президентства Дж. Буша-младшего(2001-2009 г-г);Комната 614A – помещение в здании провайдера AT&T, используемое АНБ в 2003-2006 годах для перехвата интернет-коммуникаций, основной принцип работы перехватывающего оборудования – разделение оптического сигнала, при котором 90% мощности используются в дальнейшем в коммуникационном оборудовании и 10% перенаправляются на порты мониторинга для изучения и записи.

Tailored Access Operations. Подразделение АНБ, созданное в 1997 для пассивного и активного (взломы учетных записей, установка следящего оборудования, слежка за интернет-активностью) наблюдения за

компьютерами. По данным Der Spiegel, перехватывающая способность составляет 2 петабайта данных в час. Среди используемых методов слежки: перехват ноутбуков, отправленных почтой из интернет-магазинов, перехват сообщений о случаях сбоев ОС Windows. Согласно бюджетному плану, TAO следит за 85000 устройств по всему миру, имеет базы в США и Дармштадте, ФРГ.

Boundless Informant. Система анализа, обработки, хранения и визуализации массивов Big Data для анализа глобальных электронных коммуникаций. Уже в начале 2013 года система хранила более 14 млрд. записей по Ирану, 6 млрд. – по Индии и еще 2.8 млрд. записей по США. В противоположность большинству проектов, требующих значительных финансовых вливаний в разработку ПО и инфраструктуры, BI использует готовые бесплатные open-source продукты, например, Google MapReduce и Apache Hadoop Distributed File System.

PRISM. Государственная программа и комплекс мероприятий, осуществляемых с целью негласного массового сбора информации, передаваемой сетями электросвязи, принятая АНБ в 2007. Утечка данных о существовании программы стало известно в 2013 после публикации отрывков секретной презентации в «The Guardian» и «The Washington Post». Мощность системы оценивается в 1.7 млрд. телефонных звонков и электронных сообщений и 5 млрд. записей о местонахождении владельцев мобильных телефонов в день.

Обнародование информации о PRISM вызвало рост внимания общетсвенности на технологиях PGP, шифрованном мессенджере Bitmessage и технологиях TOR.

NarusInsight. Кластерная система шпионажа, разрабатываемая компанией Boeing для американского правительства. Система состоит из большого количества компьютеров, соединённых в кластер и устанавливаемых в дата-центрах провайдеров интернета в США и Западной Европе. Система предоставляет очень широкие возможности для мониторинга, перехвата, хранения и анализа больших объёмов интернет-данных: масштабирование для анализа сверхбольших IP-сетей, real-time обработку пакетов, глубокая обработка данных искусственным интеллектом: нормализация, корреляция, агрегация и анализ, создающие ин-

формационные модели как отдельных пользователей, так и элементов информационных систем и их протоколов и приложений с возможностью анализа моделей в реальном времени; отслеживание индивидуальных пользователей и определение используемых ими программ коммуникации, высокая надёжность и отказоустойчивость, может использоваться для блокировки шифрованных сетей, построена в соответствии с законами о мониторинге пользователей CALEA и ETSI.

Tempora. Секретная программа слежения за компьютерами и коммуникационными сетями. Создана в 2011 совместными усилиями Центра правительственной связи Великобритании и АНБ. Широкой общественности стала известна в 2013 году, одновременно с PRISM. Перехваченные данные хранятся 3 дня, метаданные – более 30

MUSCULAR. Шпионская программа слежения, используемая Центром правительственной связи Великобритании (GCHQ) и АНБ, получившая известность благодаря Э. Сноудену в 2013, одновременно с PRISM и Tempora. GCHQ и АНБ используют программу для перехвата данных с серверов Yahoo! и Google. Для доступа к данным были тайно взломаны коммуникационные линии между Yahoo! и Google, объем перехвата составил несколько миллионов учетных записей и информации о владельцах. После скандала,Google заявила о начале работ над шифрованием хранимых данных.

Frenchelon. Глобальная система радиоэлектронной разведки, тайно используемая правительством Франции. Существование системы никогда не признавалось официальными лицами Франции, однако после расследования Европейского парламента появилось множество публикаций в СМИ, доказывающих наличие такой системы. Станция слежения имелись как на территории Франции, так и в заморских владениях и бывших колониях по всему миру. Основным назначением системы являлся перехват военных и дипломатических сообщений, при этом была возможность использования системы и для слежения за гражданскими лицами.

Onyx. Аналогичная Frenchelon система разведки и перехвата цифровых сообщений, действующая на территории Швейцарии. Введена в эксплуатацию в 2005 году и используется для мониторинга и хранения

гражданских и военных коммуникаций: телефон, Интернет, факс с помощью системы спутников. Весь трафик пропускается через систему фильтрации контента, основанную на списке ключевых слов. В 2006 вокруг Onyx разгорелся скандал, связанный с перехваченными с помощью этой системы дипломатическими сообщениями Египта, просочившимися в прессу. Правительство Швейцарии не подтвердило эти данные, хотя начало преследование газеты Blick за публикацию секретных документов.

Российская Федерация. В последние несколько лет тема сбора и анализа трафика граждан, в том числе перехват и анализ переписки в интернете с целью борьбы с экстремизмом, стала невероятна остра и актуальна. Далее рассмотрены основные средства анализа и хранения трафика в РФ, новейшие законопроекты и скандалы, связанные с защитой частной переписки.

СОРМ(Система технических средств для обеспечения функций оперативно-розыскных мероприятий). Согласно Закону «О связи» и приказу Министерства связи № 2339 от 9 августа 2000 г., СОРМ представляет собой «комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи». При этом необходимо различать три поколения СОРМ:

- СОРМ-1. Система прослушивания телефонных коммуникаций, организована в 1996 году.

- СОРМ-2. Система протоколирования обращений к сети Интернет. Разработана совместными усилиями ФСБ России, Госкомсвязи России, Главсвязьнадзора и ЦНИИ Связи. Организована в 2000 для прослушивания телефонных переговоров, контроля технических каналов связи.

- СОРМ-3. Система обеспечения сбора и долгосрочного хранения данных, получаемых от операторов связи, АТС, провайдеров интернет.

СОРМ обязателен для всех операторов связи в РФ, иначе возможно аннулирование их лицензии.

Конституция РФ (23 статья) допускает ограничение тайны связи только согласно решению суда, однако пункт 3 статьи 55 позволяет также ограничивать право на тайну связи, если « это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства». Также упоминается возможность использования СОРМ до получения судебной санкции в случаях, установленных федеральными законами.

Для непосредственного прослушивания разговоров требуется официальное судебное решение, однако для получения другой информации (о фактах совершения вызовов) санкции суда не требуется. Более того, сотрудники ФСБ или МВД должен получить ордер, но не обязан предъявлять его оператору связи. Также, оператор не имеет права требовать ордер, если сам не имеет допуска к государственной тайне.

Пакет Яровой. Два законопроекта, вносящие ряд поправок в закон «О противодействии терроризму» и другие акты, касающиеся этого вопроса, и в статьи Уголовного кодекса РФ, также касающиеся антитеррора. Первая часть пакета – это федеральный закон № 374-ФЗ. Данный ФЗ возлагает на операторов связи обязательство хранить и предоставлять доступ к звонкам, сообщениям и истории посещения интернет страниц своих пользователей для МВД и ФСБ. Вызвал большой общественный резонанс, так как такая база данных может попасть в третьи руки при ненадлежащем хранении и использовании. Вторая часть пакета – федеральный закон 375-ФЗ. Данный ФЗ не настолько интересен с точки зрения данной работы, т.к не предъявляет требований, которые прямо или косвенно могут привести к нарушению тайны связи, однако все равно приведем основные идеи: ужесточение ответственности за террористическую деятельность, возможность привлекать подростков от 14 лет к уголовной ответственности за терроризм, введение понятия «недоносительство».

Основная критика первого ФЗ :

- Стоимость. Создание дата-центров для хранения заявленных объ-

емов информации может стоить до 2.2 трлн рублей для «Большой тройки», при этом затраты будут возложены на абонентов, то есть реализация данного пакета приведет к увлечению стоимости мобильной связи и интернета ;

- Эффективность. Высказываются сомнения по поводу эффективности хранения такого объема данных – хотя это и может помочь расследованию совершенных преступлений, едва ли это сможет помочь в анализе шифрованного трафика, который будут использовать потенциальные злоумышленники для коммуникации;

- Потенциальные утечки. Существует вероятность, что такие базы, хранящие личные данные, в том числе цифровую переписку, множества граждан могут быть проданы или попасть в руки злоумышленников.

Требования ФСБ к мессенджерам. В марте 2018 ФСБ обязала организаторов распространения информации в сети предоставлять ключи шифрования в срок, не превышающий 10 дней. Таким образом, планируется наладить взаимодействие между силовыми ведомствами и мессенджерами с целью анализа зашифрованных сообщений и поиска потенциальных террористов. С точки зрения данной работы, требование является трудно реализуемым: некоторые мессенджеры не содержат ключей (Viber), другие же используют алгоритмы, которые делают приватные ключи недоступными (Telegram, протокол Диффи — Хеллмана). Также, существуют опасения, связанные с возможностью утечек переданных ключей и попаданием последних в третьи руки, что потенциально компрометирует крупнейшие мессенджеры и их пользователей и наносит значительный экономический ущерб владельцам мессенджеров.

На момент написания работы данный инцидент все еще не завершен, однако уже привел к конфронтации между РКН и руководством Telegram из-за технической невозможности передачи ключей к закрытым чатам.

3 Защита личной переписки

Принимая во внимание большое число угроз, рассмотрим существующие правовые и фактические способы обеспечения секретности тайны связи.

3.1 Способы защиты и ответственность в правовом аспекте

Уже упомянутый Федеральный закон «Об информации, информационных технологиях и о защите информации» вводит дисциплинарную, гражданско-правовую, административную или уголовную ответственность за нарушение интересов и прав лиц, пострадавших от разглашения информации ограниченного доступа или любого другого неправомерного использования данной информации. Подробности защиты тайны связи в России и мире рассмотрены в пункте 1.1 «Понятия в правовом аспекте»

3.2 Обзор существующего ПО для защиты переписки и его анализ

Далее рассмотрены существующие способы защиты тайны переписки в интернете с помощью существующего ПО, проведен детальный анализ и выбраны оптимальные средства для конкретных задач, т.е. оптимального баланса простоты использования, доступности и надёжности. Также рассмотрены методы защиты от угроз описанных в пункте 2.2.

Использование доверенного безопасного ПО. В первую очередь, для защиты частной переписки необходимо убедиться в использовании оригинальных программных продуктов, поставляемых надёжными поставщиками. В качестве критериев надёжности можно выбрать:

- Популярность. Если продукт находится на рынке достаточно долго, имеет хорошие отзывы и нет известных инцидентов компрометации данного продукта, то такой продукт можно считать «надёжным».
- Получение из оригинальных источников. Используемый продукт необходимо получать только от доверенного поставщика, т.е. ПО

должно быть получено от официального дистрибьютора и/или из доверенного источника (официальный сайт, репозиторий).

- Проверка на оригинальность. Для защиты от реверс-инжиниринга и/или внедрения модификации в исполнимый файл или исходный код, если продукт распространяется в таком виде, необходимо использовать валидацию полученного продукта с помощью хэш-функций, например MDA-5, SHA-256. Такой подход используется как для проприетарного (пакет Office от Microsoft), так и для open-source ПО (wine, transmission, vim). В противном случае возможно изменение ПО для превращения в кейлоггер или аналогичную программу слежения.

Средства анонимного или шифрованного общения: мессенджеры, ремейлеры, сетевые средства. Анонимные оверлейные сети – это сети, работающие поверх уже существующей и работающей сети. Рассмотрим такие примеры таких сетей:

Tor, луковая маршрутизация. Анонимная оверлейная сеть, использующая принцип «луковой маршрутизации» – технология анонимного обмена информацией, использующая многократное шифрование и пересылку шифрованных данных через цепочку частных узлов. Идеи, связанные с ЛМ, впервые появились в конце 90-х годов XX века и активно применялись ВМС США. Основной принцип работы ЛМ и Tor как частного случая: маршрутизатор при старте сессии передачи выбирает случайное число промежуточных маршрутизаторов, генерирует сообщение для каждого, шифруя их симметричным ключом и указывая для каждого маршрутизатора, какой маршрутизатор будет следующим на пути (структура, аналогичная односвязному списку); для получения симметричного ключа устанавливается начальное соединение с каждым промежуточным маршрутизатором и используется его открытый ключ; таким образом, передаваемые по сети сообщения имеют «луковую» структуру, где для получения доступа к содержимому сообщения необходимо поочередно «снимать слои» ; каждый маршрутизатор «снимает один слой», получает предназначенные только ему указания маршрутизации (следующий прокси) и шифрованное сообщение, которое

необходимо передать далее; последний маршрутизатор «снимает последний слой», отправляет сообщение адресату. Таким образом формируется устойчивая сеть, где каждый прокси передает сообщения в любую сторону, наращивая слои шифрования при передаче ответного сообщения.

Преимущества Tor и луковой маршрутизации:высокая степень несвязности сети, прямо зависящая от кол-ва участвующих прокси; возможность работы даже при наличии скомпрометированных узлов, если только вся сеть не стоит из таких узлов; сочетание Tor и других средств шифрования и анонимности позволяет бороться с PRISM.

Недостатки: отсутствие защиты от анализа синхронизации в слабонагруженных сетях, отсутствие защиты от анализа данных, проходящих через выходные узлы, т.к. оператор может получить доступ к данным через сниффинг, если только не используется конечная криптография типа SSL/TSL; уязвимости к атакам MITM, по времени, по сторонним каналам, глобальному пассивному наблюдению; ошибки в программной реализации; на последнем узле цепи Tor возможна деанонимизация отправителя или модификация отправляемого сообщения; при работе с сетью к сообщениям пользователя может добавляться техническая информация, полностью либо частично раскрывающая отправителя.

Чесночная маршрутизация, I2P.I2P – проект, начатый с целью создания анонимной компьютерной сети, работающей поверх сети интернет. Создатели проекта разработали свободное программное обеспечение (ПО), позволяющее реализовать сеть, работающую поверх сети интернет. Такая сеть является оверлейной, устойчивой к отключению узлов, шифрованной и анонимной к определению IP-адресов. Внутри сети возможно размещение любого сервиса или службы: файлообменник, электронную почту, форум, чат, VoIP) при полном сохранении анонимности сервера. I^2P допускает построение одноранговых сетей типа BitTorrent, Kad, Gnutella. Сеть является самоорганизующейся и распределённой, используется модифицированный DHT Kademlia, при этом сеть хранит хешированные адреса узлов сети, зашифрованные AES-протоколом IP-адреса и публичные ключи шифрования, при этом соединения по Network database тоже зашифрованы. Сеть предоставляет приложениям транспортный механизм для анонимной и защищённой

пересылки сообщений друг другу. Благодаря библиотеке Streaming lib реализована доставка пакетов в первоначально заданной последовательности без ошибок, потерь и дублирования, что даёт возможность использовать в сети I2P IP-телефонию, интернет-радио, IP-телевидение, видеоконференции и другие потоковые протоколы и сервисы. Внутри сети существует автономный каталог сайтов, электронные библиотеки,торрент-трекеры. Также существуют шлюзы для доступа в сеть I2P непосредственно из Интернета, созданные для пользователей, которые не могут установить на компьютер программное обеспечение «Проекта Невидимый Интернет». Внутри I2P реализованы механизмы шифрования, P2P (peer to peer)-архитектура, перемены посредников (хопы).

Преимущества: сеть изначально проектировалась с предположением скомпрометированности всех промежуточных узлов, весь трафик шифруется от отправителя до получателя с использованием четырёх уровней шифрования (сквозное, чесночное, туннельное, шифрование транспортного уровня), добавляется небольшое случайное количество случайных байт; все пакеты зашифровываются на стороне отправителя и расшифровываются только на стороне получателя, при этом никто из промежуточных участников обмена не имеет возможности перехватить расшифрованные данные и никто из участников не знает, кто на самом деле отправитель и кто получатель; сеть устойчива к потере даже значительного (более 50%) числа узлов и попыткам внешнего анализа.

Недостатки: уязвимость к подмене узлов, при которой злоумышленник заменяет рабочие узлы на скомпрометированные; перехвата туннелей; атака методом исключения, при которой злоумышленник последовательным перебором может установить, какие маршрутизаторы используются конкретным пользователем; Sybil attack, позволяющая без захвата контроля над узлом закрыть доступ узлам сети к определённой информации; низкая скорость доступа, для синхронизации с сетью требуется примерно час.

JonDo. ПО, предоставляющее доступ к цепочке прокси-серверов, напоминающее Tor. В отличии от Tor, где ноду может создать любой участник, JonDo опирается на помощь отдельных организаций и группировок. К недостаткам относятся все уязвимости Tor, низкая скорость

доступа, сильно ограниченное число нод.

Ремейлеры представляют собой серверы, пересылающие сообщения электронной почты по указанному адресу. Делятся на псевдонимные и анонимные. Последние делятся на ремейлеры шифропанков, MixMaster, MixMinion. При использовании псевдо-анонимного ремейлера, его оператор знает адрес электронной почты, который необходим для получения ответа на письмо. Тайна связи полностью зависит от оператора, который может стать жертвой угроз, шантажа или социальной инженерии. Преимуществом псевдо-анонимных ремейлеров является их юзабилити, за которое пользователь расплачивается меньшей защищённостью. Анонимные ремейлеры обеспечивают гораздо более высокую секретность, но при этом они и сложнее в использовании. Их операторы не могут знать, какие данные пересылаются через них, а поэтому нет гарантии своевременной доставки сообщения, которое может и вовсе затеряться.В обмен на высокое время ожидания анонимные ремейлеры достаточно надёжно скрывают от посторонних глаз реальный адрес и содержимое сообщения.

- Ремейлеры шифропанков удаляют из полученных писем всю информацию, которая может быть использована для идентификации отправителя, и пересылают письмо на указанный адрес. Чаще всего используется PGP-шифрование, возможно создание цепочки таких ремейлеров.

- MixMaster. Требуют установки и более совершенны, чем прошлый тип, т.к отправляемые сообщения всегда константного размера, что делает невозможной отслежу по размерам.

- MixMinion. Стандарт реализации третьего типа протокола анонимной пересылки электронной почты, может отсылать и принимать анонимные сообщения электронной почты, основан на пересылаемых защищённых одноразовых блоках.

Ремейлеры также имеют ряд уязвимостей и недостатков: тэговая атака, атака на выходные узлы, DDoS, путь доставки сообщений не всегда является оптимальным.

Стеганография. Способ тайной передачи информации путем сохранения в тайне самого факта передачи информации. В отличие от

криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Термин введен в конце XV века монахом Иоганном Тритемием в трактате «Steganographia», зашифрованном под магическую книгу. Криптография защищает содержание сообщения, стеганография – сам факт наличия каких-либо скрытых посланий. Существует множество аналоговых методов стеганографии, однако в контексте данной работы рассматриваются только цифровые методы. **Цифровая стеганография** — направление стеганографии, основанное на сокрытии и/или внедрении дополнительной информации в цифровые объекты, вызывая при этом искажения этих объектов. Как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, находящихся вне порога чувствительности среднестатистического человека, не приводит к значительным изменениям этих объектов. Также, в оцифрованных объектах, первоначально имеющих аналоговую природу, всегда присутствует шум квантования. Существующие алгоритмы цифровой стеганографии:

- Сетевая стеганография, основанная на использовании особенностей работы сетевых протоколов передачи данных, когда части отдельных пакетов заменяются битами секретной информации.

- Встраивание в изображение, при этом алгоритм работает непосредственно с цифровым сигналом (LSB), накладывает (fusion) изображение поверх существующего (цифровые водяные знаки), использование особенностей файлов (хранение в метаданных или неиспользуемых полях).

- Эхо-методы аудио-стеганографии, использующие неравномерные промежутки между эхо-сигналами для кодирования последовательности значений.

Необходимо помнить, что если алгоритм стеганографии или используемое ПО станут известны аналитику, анализ может быть проведен за

адекватное время, поэтому перед кодировкой сообщений их необходимо шифровать с помощью криптографии.

В целом, стеганография является качественным методом для передачи небольших (по сравнению с файлом, в который происходит встраивание) текстовых сообщений или мультимедиа объектов. Однако, стеганография не имеет широкой популярности и имеет уязвимости: атака на основании известного заполненного контейнера, на основании известного встроенного сообщения, на основании выбранного встроенного сообщения, на основании известного пустого контейнера, на основании выбранного пустого контейнера, на основании известной математической модели контейнера или его части.

Мессенджеры. Наиболее классическая и очевидная область применения существующих наработок в области защиты тайны связи, т.к. содержат преимущественно частную переписку, подвергающуюся анализу со стороны злоумышленников и государств. Ниже рассмотрены самые популярные мировые мессенджеры (РФ в целом следует европейским трендам).

Viber. Первый по популярности мессенджер в РФ. В 2016 году Viber получил сквозное (end-to-end) шифрование, однако подробности работы, например, симметричность или асимметричность, метод распределения ключей. При этом через шифрование проходят как текстовые, так и мультимедийные объекты, пересылаемые в диалогах.ля этого каждый из клиентов использует открытый и закрытый ключ. Их генерирование осуществляется автоматически в момент установки программы на устройствах обеих сторон, что является потенциальной уязвимостью, так как ключи не уникальны для каждого диалога.Существует мнение, что «поскольку и алгоритмы шифрования, и ключи шифрования, и уже расшифрованные сообщения находятся внутри софта мессенджера на конечном устройстве, доступ к любой информации у владельца мессенджера может быть» и Viber не является в этом отношении исключением, кроме того «Viber компрометируют себя функцией создания копий истории переписки». Более того, имел место инцидент со взломом одного из вспомогательных сервисов Viber Support в 2013 году группировкой «Syrian Electronic Army». В 2015, согласно Закону « О персональных данных»,

требующего хранения персональных данных россиян на территории РФ, Viber принял решения о переносе номеров телефонов и никнеймов на территорию РФ, предоставив доступ правоохранительным органам. Были высказаны опасения, что дата-центры могут быть атакованы злоумышленниками на территории РФ, что потенциально ведет к значительной утечке данных.

WhatsApp. Второй по популярности мессенджер в РФ. По состоянию на март 2015 года ежедневный объем трафика составлял 50 млрд. сообщений. WhatsApp использует модифицированный протокол XMPP, при установке создаётся аккаунт на сервере s.whatsapp.net, использующий номер телефона в качестве имени пользователя, порт под Android автоматически использует в качестве пароля MD5-хеш от изменённого идентификатора IMEI, а версия под iOS – MD5-хеш от MAC-адреса. Из-за такого слабого алгоритма генерации пароля (MD5 содержит множество доказанных уязвимостей и коллизий) и отсутствия шифрования, WhatsApp подвергался критике.

С апреля 2016 мессенджер получил технологию сквозного шифрования. Шифрование распространяется на все типы сообщений: текст, фото, видео и голосовые сообщения. Шифрование также доступно в групповых чатах.В 2017 года стало известно, что в системе шифрования сообщений был обнаружен бэкдор, позволяющий компании Facebook скрытно изменять ключи шифрования и потребовать от приложения-отправителя перешифровать сообщения на новых ключах, а затем повторно отправлять их (при включённой настройке «Show Security Notifications» отправитель увидит уведомление о подобном факте после перешифрования сообщений). Фактически эта функциональность позволяет серверам Facebook перехватывать и расшифровывать сообщения пользователей. Обнаруживший данную уязвимость исследователь обратился в Facebook в 2016 году, но получил ответ, что данная функциональность известна авторам системы и является «ожидаемым поведением». Представитель компании пояснил, что возможность перешифровки сообщений необходима, так как часть пользователей часто меняет телефоны и сим-карты, а компания принимает меры, чтобы даже в таких случаях отправленные сообщения были доставлены получателям.

Telegram. Мессенджер не входит в тройку самых популярных, однако реализует некоторые оригинальные технологии и породил много общественного резонанса. Итак, Telegram — кроссплатформенный мессенджер, позволяющий обмениваться сообщениями и медиафайлами многих форматов , использующий закрытую проприетарную серверную часть и несколько версий открытых клиентов, доступных под лицензий GNU GPL. Telegram приобрел значительную популярность в связи с высказываниями владельца, Павла Дурова, о полной защищенности от прослушивания секретных чатов данного мессенджера.

В основе коммуникации лежит протокол MTProto, предполагающий использование нескольких протоколов шифрования. Для авторизации и аутентификации используются алгоритмы RSA-2048, DH-2048 для шифрования, при передаче сообщений протокола в сеть они шифруются AES с ключом, известным клиенту и серверу. Также применяются криптографические хеш-алгоритмы SHA-1 и MD5. С 2013 года появился режим «секретных» чатов (Secret Chats). Такой режим реализует шифрование, при котором только отправитель и получатель обладают общим ключом (end-to-end), применяется алгоритма AES-256 в режиме Infinite Garble Extension для пересылаемых сообщений. Отличия данного режима работы от классического заключается в том, что сообщения не расшифровываются сервером, а только пересылаются через него, сами сообщения хранятся на устройствах в зашифрованном виде. Протокол допускает использование шифрования end-to-end с опциональной сверкой ключей, используется протокол Диффи-Хэлмана для обмена 2048-битными RSA-ключами между двумя устройствами и ряд хеш-функций.

В июне 2017 года Роскомнадзор публично направил обращение Павлу Дурову с требованием предоставить информацию о компании для последующего внесения мессенджера Telegram в Реестр организаторов распространения информации в сети: полное и сокращенное наименование, страна регистрации, налоговый идентификатор и/или идентификатор в торговом реестре страны регистрации, адрес местонахождения, почтовый адрес, электронный адрес, доменное имя, электронный адрес администратора ресурса, провайдера хостинга и описание сервиса, предоставляемой услуги. После отказа предоставить данные, Дуров офици-

ально был предупрежден о возможности блокировки Telegram на территории РФ. Позже мессенлжеру было предъявлено требование предоставить ФСБ ключи для расшифровки обычных и секретных чатов, на что получили отказ, связанный с невозможностью предоставить ключи к секретным чатам, связанную с особенностями работы MTProto. С 16 апреля 2018 года РКН начал блокировку мессенджера на территории РФ.

Преимущества: высокий уровень анонимности, доступность в заблокированных странах, постоянное внедрение новых технологий передачи данных и защиты сообщений.

Недостатки: до 16 версий протокола была возможность атаки повтором, состоящей в необходимости доверять серверу номера сообщений, что приводило к возможности повторной передаче сообщений злоумышленником и создавало возможность анализа ответов сервера и других абонентов; timing-атака, использующая временной интервал между отправкой сообщения и приеме ответа об ошибке; по данным публикаций, протокол не имеет authenticated encryption и indistinguishability under chosen-ciphertext attack, что делает возможным две атаки:

- Атака с увеличением длины сообщения. К сформированному шифротексту $C = \{tags, y_1, y_2, ..., y_l\}$, который дешифруется в сообщение $X = \{tags, message, padding\}$ добавляется новый блок 128 бит, т.е принимаемый шифротекст принимает вид $C' = \{tags, y_1, y_2, ..., y_l, r\}$, где r – добавочный блок 128 бит. Сообщение расшифровывается как $X' = \{tags, message, padding'\}$, в котором $padding' = \{padding, padding^*\}$ и длинна$padding'$ больше длины блока. Т.к длинна $padding$ не проверяется, дешифрование пройдет успешно. Для предотвращения данного типа атаки необходимо лишь проверять длину блока padding, в случае превышения допустимого размера необходимо прекращать дешифрование сообщения.

- Атака с изменением последнего шифрованного блока. В сформированном шифротексте $C = \{tags, y_1, y_2, ..., y_l\}$, дешифруемом в сообщение $X = \{tags, message, padding\}$, изменяется последний блок и принимаемое сообщение C принимает вид $C' = \{tags, y_1, y_2, ..., y_{l-1}, r\}$. Таким образом, измененное сообщение расшифровывается как $X' =$

$\{tags, message', padding'\}$ и длина $padding'$ равна длине $padding(p)$. С вероятностью 2^{-32} дешифрованное сообщение совпадает с оригинальным. Для предотвращения такого типа атаки, необходимо добавить тег проверки padding в заголовки отправляемого сообщения.

По итогам обзора существующего ПО, рекомендуется использовать стеганографию для отправки небольших текстовых сообщений и мультимедиа, I^2P для анонимных форумов и хостингов или одноранговых сетей типа BitTorrent и Telegram (как только будет решен конфликт с РКН или при условии вне РФ) для повседневных коммуникаций и аудиосвязи через интернет.

3.3 Защита от основных видов угроз в частном секторе

Далее будут рассмотрены методы защиты от основных угроз существующих в частном секторе и рассмотренных в пункте 2.2.

SpyWare. Если угроза со стороны SpyWare становится более чем назойливой, существует ряд методов для борьбы с ними. Среди них программы, разработанные для удаления или блокирования внедрения SpyWare, также как и различные советы пользователю, направленные на снижение вероятности попадания SpyWare в систему. В случае значительной степени инфицированности ОС SpyWare наиболее действенным способом борьбы является сохранение данных пользователя (необходимо убедиться, что данные не заражены) и полная переустановка ОС. Также можно выделить методы по предотвращению заражения устройства: использование файрволов и прокси-серверов для блокировки доступа к сайтам, известным как распространители spyware, использование hosts-файла, препятствующего возможности соединения компьютера с сайтами, известным как распространители spyware, скачивание программ только из доверенных источников (предпочтительно с веб-сайтов производителя), поскольку некоторые spyware могут встраиваться в дистрибутивы программ, использование антивирусных программ с максимально «свежими» вирусными базами. Т.к основной целью SpyWare является

конфиденциальная информация, рекомендуется использование одноразовых паролей/двухфакторная аутентификация, использование систем проактивной защиты, использование виртуальных клавиатур (неактуально для ПО, делающего снимки экрана).

MITM. Основное решение – использование стойкого шифрования между клиентом и сервером. В таком случае сервер может идентифицировать себя посредством предоставления цифрового сертификата, после чего между пользователем и сервером устанавливается шифрованный канал для обмена конфиденциальными данными. Но в этом случае возникает зависимость от самого сервера и выбора им метода шифрования. Другим вариантом защиты от некоторых видов MITM-атак является полный отказ от использования открытых Wi-Fi-сетей для работы с личными данными. Хорошую защиту дают некоторые плагины для браузеров. Например, «HTTPS Everywhere» или «ForceTLS», которые самостоятельно устанавливают защищенное соединение всякий раз, когда эта опция доступна на стороне сервера.

Защита от атак на криптографические протоколы. Детальный разбор всех средств защиты от существующих методов атак лежит далеко за границами данной работы, тем не менее ниже рассмотрены самые распространенные способы борьбы с угрозами из пункта 2.2.

Для защиты от атаки подменой используется привязка ключей к обоим контрагентам, идентификаторы которых передаются друг другу в шифрованном, обычно, хэш-функцией, виде. Для защиты от replay attack используется построение криптостойкой системы аутентификации. Основная идея состоит в том, что каждая сессия аутентификации использует оригинальные параметры (ключи) : метка времени создания ключа, случайное число, одноразовые коды. Защита от атак с использованием специально подобранных текстов подразумевает включение случайных чисел в post-get запросы и использование протоколов с нулевым разглашением – интерактивный криптографический протокол, позволяющий одной из взаимодействующих сторон убедиться в достоверности какого-либо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны. Для защиты от known-key атаки обеспечивают независимость между различными применяемыми ключа-

ми, достигаемой с помощью протоколов совместной выработки ключа, не позволяющего ни одной стороне узнать ключ по существующим данным до выработки совместного ключа. И наконец, для зашиты от атак, использующих особенности специфику данного протокола, необходимо провести анализ существующей архитектуры, найти «бутылочные горлышки», использовать более надёжные генераторы случайных чисел, передавать данные с хэш-«солью».

3.4 Реализация собственного программного продукта

В качестве собственного ПО для защиты тайны переписки предлагается реализация модифицированного алгоритма BLOWFISH – криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа, разработанный Брюсом Шнайером в 1993 году и представляющий собой сеть Фейстеля – один из методов построения блочных шифров, в котором сеть состоит из ячеек, называемых ячейками Фейстеля; на вход каждой ячейки поступают ключ и данные, а на выходе каждой ячейки получают изменённые данные и изменённый ключ, при этом все ячейки однотипны и сама сеть представляет собой определённую итерированную (многократно повторяющуюся) структуру; ключ выбирается в зависимости от алгоритма шифрования/дешифрования, меняется при переходе между ячейками. При шифровании/ дешифровании выполняются одни и те же операции, а отличается только порядок ключей.

Алгоритм выбран по причине простоты реализации, сравнительно высокой устойчивости и высокой скорости работы. Алгоритм выполнен на быстрых и простых для CPU операциях: сложение, подстановка и XOR (исключающее или).

Описание алгоритма. Алгоритм состоит из двух частей: расширение ключа и шифрование данных. На этапе расширения ключа исходный ключ (длиной до 448 бит) преобразуется в 18 32-битовых подключей и в 4 32-битных S-блока, содержащих 256 элементов. Общий объём полу-

ченных ключей равен $(18+256*4)*32=33344$ бит, т.е 4168 байт.

Параметры алгоритма: секретный ключ K от 32 до 448 бит, 32-битные таблицы S_1-S_4, каждая по 225 элементов длиной; 32-битные шифрующие ключи P_1-P_{18}.

Функция F(x), приминающая на вход блок в 32 бита и совершающая преобразование: 1.32-битный блок делится на четыре 8-битных блока $X_1...X_4$, каждый из которых – индекс массива таблицы замен S_1-S_4. 2. Значения $S_1[X_1]$ и $S_2[X_2]$ складываются по модулю 2^{32}, складываются по модулю 2 с $S_3[X_3]$ и складываются также с $S_4[X_4]$. 3. Результат этих операций и есть значение $F(x)$.

Алгоритм шифрования 64-битного блока с известным массивом P и F(x). Blowfish представляет собой Сеть Фейстеля, состоящую из 16 раундов. Алгоритм шифрования блока X размером 64 бит выглядит следующим образом: 1.Разделение входного блока X на 2 32-битных блока L_0,R_0. 2. Для $i=1;16$: $L_i=L_{i-1}+P_i; R_i=R_{i-1}+F(L_i)$. 3. После 16 раунда L_{16},R_{16} меняются местами, к получившимся блокам прибавляются P_{17},P_{18}. 4. Выходной блок Y = конкатенации L_{17},R_{17}.

Непосредственно алгоритм разделен на 2 этапа:

1. Подготовительный — формирование ключей шифрования по секретному ключу.

- Инициализация массивов P и S при помощи секретного ключа K : 1.Инициализация P_1-P_{18} фиксированной строкой, состоящей из шестнадцатеричных цифр мантиссы числа Пи (могут быть выбраны любые другие значения:цифры числа e, RAND-таблицы или биты с выхода генератора случайных чисел);2.Производится операция XOR над P_1 с первыми 32 битами ключа K и т.д. Если ключ K короче, то он накладывается циклически.

- Шифрование ключей и таблиц замен. 1.Алгоритм шифрования 64-битного блока, используя инициализированные ключи P_1-P_{18} и таблицу замен S_1-S_4, шифрует 64-битную нулевую (0x0000000000000000) строку. Результат записывается в P_1,P_2. 2. P_1,P_2шифруются изменёнными значениями ключей и таблиц замен. Результат записывается в P_3,P_4. 3. Шифрование продолжается до изменения всех ключейP_1-P_{18} и таблиц замен S_1-S_4.

2. Шифрование текста полученными ключами и F(x), с предварительным разбиением на блоки по 64 бита. Если невозможно разбить начальный текст точно на блоки по 64 бита, используются различные режимы шифрования для построения сообщения, состоящего из целого числа блоков. Суммарная требуемая память 4168 байт.

Дешифрование происходит аналогично, только $P_1 - P_{18}$ применяются в обратном порядке.

Криптостойкость. Вероятность появления слабого S-блока равна 2^{-15}. Невозможно заранее определить, является ли ключ слабым. Проводить проверку можно только после генерации ключа. Криптостойкость можно настраивать за счёт изменения количества раундов шифрования (увеличивая длину массива P) и количества используемых S-блоков. При уменьшении используемых S-блоков возрастает вероятность появления слабых ключей, но уменьшается используемая память. Адаптируя Blowfish для 64-битной архитектуры, можно увеличить количество и размер S-блоков (а следовательно и память для массивов P и S), а также усложнить F(x), причём для алгоритма с такой функцией F(x) невозможны вышеуказанные атаки. Известно, что вариант Blowfish с уменьшенным количеством раундов является уязвимым к атаке на основе открытых текстов на сравнительно слабых ключах. Реализации Blowfish с 16 раундами шифрования не подвержены подобным атакам.

Test