

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	3
1 Понятия «тайна связи» и «личная переписка» в правовом и информационном аспектах	5
1.1 Понятия в правовом аспекте	5
2 Понятие «цифровой угрозы» , новые цифровые угрозы . .	9
2.1 Определение	9
2.2 Основные виды, угрозы в частном секторе	9
2.3 Государство как атакующая сторона	14
3 Защита личной переписки	17
3.1 Способы защиты и ответственность в правовом ас- пекте	17
3.2 Защита переписки при помощи существующего ПО	17
Список использованной литературы	18

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, участвовавшими 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 частных 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 правовом и информационном аспектах

1.1 Понятия в правовом аспекте

Так как все пользователи информационных систем являются в первую очередь гражданами правовых государств и объектами и субъектами права, рассмотрение основных понятий начнём с правового 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/ЕС) пришел General Data Protection Regulation, GDPR (Общеввропейский 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 получают 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, угрозы 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 обнаруживаемость 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 приоритетом 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 middle», MITM). В основе такой атаки лежит перехват сообщений на линии коммуникации между отправителем и абонентом. 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 прочесть или модифицировать, не взломав ключ шифрования или не используя 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, зашифрованное 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 А открытый ключ стороны В и у стороны В открытый ключ А. 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 (криптоаналитик) 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 Государство как атакующая сторона

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.

ки.

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 таможи, возможность покупки билетов на самолеты и поезда, право на обучение детей в частных дорогих школах.

США. 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: **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 614А – 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.

text

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.

3.2 Защита переписки при помощи существующего ПО

Test