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).

2.2 Основные виды

Основными видами угроз являются утечки и перехваты сообщений, происходящие с помощью SpyWare (подмножество вирусов), целенаправленных атак на протоколы и средства связи, 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 ра-

ботой 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 состояния 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.

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