

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 (Перенос?) кафедры прикладной математики В. А. Лушников

Симферополь 2018

Оглавление

Введение	3
1 Понятия «тайна связи» и «личная переписка» в правовом и информационном аспектах	4
1.1 Понятия в правовом аспекте	4
2 Защита личной переписки	6
2.1 Способы защиты в правовом аспекте	6
Список использованной литературы	6

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 киберпреступниками 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 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.» Исходя из данного закона, в дальнейшем под **«тайной связи»** будет подразумеваться совокупность тайны переписки, телефонных разговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Также, в дальнейшем к сетям электросвязи будем относить и Интернет.

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

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 проведения 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 правоохрательными органами прослушивающего оборудования без соответствующих санкций (ордера) суда или другие действия, выходящие за рамки полномочий правоохрательных 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 Защита личной переписки

2.1 Способы защиты в правовом аспекте

Test