УДК 004.773

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ОБЩЕНИЯ В ИНТЕРНЕТЕ

Коршунов И.Е., Васильев С.С.
Руководитель: педагог МБОУ ДОД ЦДТТ Усачев С.В.
Муниципальное бюджетное образовательное учреждение дополнительного образования детей «Центр детского технического творчества»

Цель : выявить возможные уязвимости при общении в интернете и способы их устранения.

Задачи :

1. Исследовать литературу.
2. Провести анализ полученной информации.
3. Разработать свой способ повышения уровня безопасности при общении в интернете.

Актуальность : кто владеет информацией - тот владеет миром, а значит всегда будут люди жаждущие любыми способами получить к ней доступ. В современном мире очень многое связывает человека с электронными устройствами. Мы храним и обрабатываем информацию на компьютерах, общаемся через интернет, используем мобильную связь. Все это, безусловно, упрощает жизнь. Нет необходимости преодолевать большие расстояния, что бы передать человеку какую - либо информацию, не нужно хранить стопки рукописных бумаг. Но не все так хорошо, как хотелось бы. Использование электронных устройств упрощает повседневную жизнь, но вместе с тем и увеличивает риск утечки данных в руки злоумышленников. Одна из важных проблем современной информатики - обезопасить передачу и хранение информации.

Чтобы убедиться в актуальности этой темы, мы провели опрос, участникам которого были заданы следующие вопросы:

1. Допускаете ли вы, что вашими личными данными (переписками) в интернете могут завладеть злоумышленники?
2. Хотели бы вы получить возможность безопасного общения в интернете?

В опросе приняло участие 83 человека, его результаты представлены на диаграммах:

Результаты опроса показывают, что, несмотря на меры предосторожности (создание сложных паролей и т.д.), люди обеспокоены тем, что в любой момент кто - то может завладеть их личной информацией (переписками), что подтверждает актуальность данной проблемы.

Возможные способы утечки информации : так как тема безопасности в интернете слишком велика, мы рассмотрим именно безопасность общения через интернет.

На сегодняшний день существует довольно много сервисов и приложений, которые предоставляют возможность общения в интернете, наиболее распространенными в настоящее время являются социальная сеть Вконтакте и приложение Skype.

Казалось бы, у нас уже есть довольно много сервисов, которые гарантируют нам высокий уровень безопасности и защиты от так называемых "мошенников", зачем же создавать что-то новое?

Ответ довольно прост. Эти приложения и сервисы не настолько безопасны насколько хотелось бы, у каждого есть свои уязвимости, которыми может воспользоваться злоумышленник.

В этом разделе мы рассмотрим общие уязвимости для всех сервисов:

1. Перехват сообщений.
2. Утеря пароля.
3. Переход по вредоносным внешним ссылкам.
4. Взлом.

Основные способы защиты :

1. Создание сложных паролей (длинные пароли, содержащие буквы разного регистры, цифры и спецсимволы).
2. Установка дополнительного ПО (антивирусы).
3. Игнорирование вредоносных ссылок.
4. Игнорирование сообщений от сомнительных пользователей.
5. Не устанавливать сомнительные программы на свой компьютер
6. Ни кому не сообщать свои логины и пароли от социальных сетей и почтовых сервисов.

Сравнение популярных сервисов для общения в интернете: Вконтакте, Skype и нашей программы: мы провели сравнение нашего продукта с наиболее распространенными сервисами для общения, а именно ***Skype*** и социальной сетью ***Вконтакте***, с результатами сравнения можно ознакомиться в таблице.

	Вконтакте	***Skype***	***Наша программа***
Привязка к мобильному телефону/почте	+	+	-
Шифровка отправляемых сообщений	-	+	+
Хранение переписок на сервере	+	-	-
Передача сообщений (и ключа) на несколько устройств при параллельной сессии	+	+	-

Как можно заметить, разработанная нами программа имеет ряд преимуществ в обеспечении безопасности личной информации перед своими конкурентами.

Более подробно о преимуществах нашего продукта :

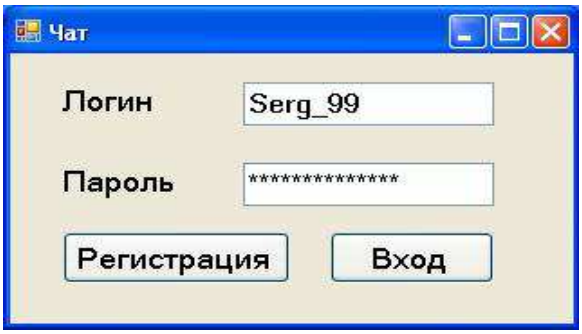
1. Отсутствие привязки учетной записи, к каким-либо личным данным обеспечивает полную анонимность и защиту от получения злоумышленниками личных данных (телефонного номера, электронной почты и т.д.).

2. Шифровка сообщений происходит автоматически при отправке сообщений (расшифровка при получении), в отличие от ***Skype*** мы предоставляем право пользователю самостоятельно придумать ключ, по которому будут шифроваться сообщения (указывается для каждого пользователя в отдельности), что позволяет в любой момент сменить его и исключить возможность прочтения человеком перехватившим сообщение.

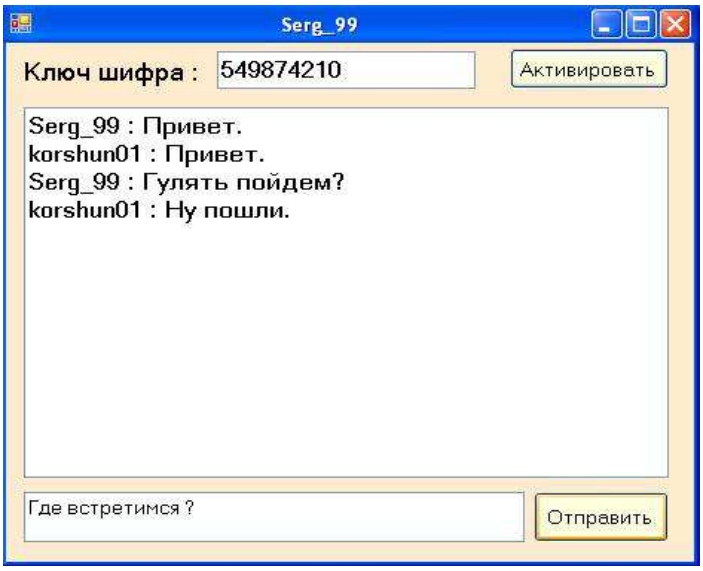
3. Хранение сообщений происходит на клиенте (в случае если пользователь решит этим воспользоваться), а значит, исключается вероятность того, что в случае взлома сервера будут утеряны переписки всех пользователей.

4. Одновременно с одной учетной записи может авторизоваться всего один пользователь, если злоумышленник войдет под вашим логином и паролем, он не сможет воспользоваться вашими перепиской, потому что они не хранятся на сервере и не высылаются при входе, так же он не сможет вести диалог с другими пользователями из-за отсутствия ключа, в связи с чем пропадает смысл взлома (в случае ***Skype*** высылается ключ для расшифровки сообщений и становится видна вся переписка, при параллельном входе все сообщения дублируются в режиме реального времени).

Принцип работы программы :



1. Пользователь авторизируется в сети.
2. На сервер отправляются IP адрес, который хранится, пока пользователь в сети.
3. В поле поиска собеседника вводится логин собеседника и отправляется запрос на сервер, который связывает нас с этим пользователем, дальше общение происходит напрямую между пользователями.
4. Открывается окно диалога, в котором необходимо ввести ключ шифровки сообщений (обговаривается собеседниками заранее).
5. В поле ввода вводится текст сообщения, при нажатии на кнопку "Отправить" программа производит шифровку сообщения (согласно введенному ключу) и отправляет собеседнику.



6. При получении происходит расшифровка сообщения (по введенному ключу), после чего выводится в поле диалога.

Области применения :

1. Приватное общение с собеседниками.
2. Корпоративное общение, с целью обезопасить обсуждаемые секреты компании.

Вывод: мы выявили основные уязвимости при общении в интернете и разработали безопасную программу для общения в интернете.