УДК 004.056

ОЦЕНКА БЕЗОПАСНОСТИ СИСТЕМ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ МЕТОДОМ АНАЛИЗА ИЕРАРХИЙ

SAFETY ASSESSMENT OF THE SYSTEMS OF INSTANT MESSAGING BY THE METHOD OF ANALYSIS HIERARCHIES

З.А. Внукова, А.Д. Буханцов, Н.П. Путивцева, С.И. Кулешов
Z.A. Vnukova, A.D. Bukhantsov, N.P. Putivceva, S.I. Kuleshov

Белгородский государственный национальный исследовательский университет, Россия, 308015, Белгород, ул. Победы, 85

Belgorod State National Research University, 85 Pobeda St, Belgorod, 308015, Russia

e-mail: 1002751@bsu.edu.ru, bukhantsov@bsu.edu.ru, putivzeva@bsu.edu.ru, Kulechov27@mail.ru

Аннотация. В данной статье рассмотрены основные характеристики наиболее популярных из представленных на современном рынке систем мгновенного обмена сообщениями, определяющих конфиденциальность пользовательских данных и обеспечивающих тайну переписки, телефонных переговоров и иных сообщений. На основе метода анализа иерархий Т. Саати для принятия решений в данной работе предлагается набор альтернатив современных систем мгновенного обмена сообщениями, для которого были выявлены основополагающие критерии оценки безопасного обмена информацией. В ходе исследования был определен круг приложений-мессенджеров, наиболее соответствующих выбранным критериям оценки. Полученные результаты являются основой для формирования системы критериев сравнительной оценки мессенджеров и обоснования их выбора не только с точки зрения безопасности, но и для других возможных целей.

Resume. This article describes the main characteristics of the most popular instant messaging systems known on the market today that determine the confidentiality of user data and able to ensure the privacy of correspondence, telephone conversations and other communications. Based on method analytic hierarchy process of T. Saati, this paper proposes a set of alternatives to modern instant messaging, for which were identified the basic criteria of evaluation the secure exchange of information. During the research was identified the list of applications, instant messengers, the most relevant selected evaluation criteria. Received results are the basis for creation of a criteria system of comparative evaluation messengers and justification a choice, not only in terms of security regulations, but also for other possible objectives.

Ключевые слова: анализ, безопасность, мессенджер, чат, протокол шифрования, защита информации.

Keywords: analysis, security, messenger, chat, encryption protocol, data protection.

Теоретический анализ

Информация в современном обществе служит не только предметом профессиональных интересов, но и ресурсом принятия решений, средством обеспечения более высокого качества жизни. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих общей безопасности людей. Одним из элементов современных технологий информационного обмена являются так называемые мессенджеры, которые активно используются наряду с электронной почтой, sms-сообщениями и другими технологиями передачи данных.

Системы мгновенного обмена сообщениями, мессенджеры (от англ. messenger — курьер), представляют собой службы мгновенных сообщений для обмена информацией в режиме реального времени через Интернет: текстовые сообщения, звуковые сигналы, изображения, видео. Некоторые из них предоставляют такие услуги, как игры, групповые текстовые чаты или видеоконференции.

Проблема обеспечения безопасности обмена данными на таких открытых ресурсах, как системы мгновенного обмена сообщениями, достаточно актуальна. Информация все чаще выполняет функции объекта преступных посягательств, средства конкурентной борьбы в бизнесе, политике и даже оружия информационных войн [Жукова и др., 2015]. В этих условиях активно возрастает роль безопасного использования информации, в том числе и в повседневной жизни каждого человека.

Для анализа и выбора наиболее безопасных мессенджеров был применен метод анализа иерархий (МАИ), созданный американским математиком Т. Саати в конце 1970-х. Суть этого метода состоит в декомпозиции проблемы или цели на более простые составляющие части и в поэтапном установлении приоритетов оцениваемых компонент с использованием парных сравнений. При этом проблема принятия решения представляется в виде иерархически упорядоченных:

1. главной цели (главного критерия) рейтингования возможных решений,
2. нескольких групп (уровней) однотипных факторов, так или иначе влияющих на рейтинг,
3. группы возможных решений,
4. системы связей, указывающих на взаимное влияние факторов и решений.

МАИ часто используется для оптимизации функционирования систем поддержки принятия решений [Фурцев, Коваленко, Ткаченко, 2014]. Однако, данный подход можно применить и для сравнительной оценки уровня безопасности систем мгновенного обмена сообщениями.

Исследование и его результаты

В данном исследовании была построена наиболее простая иерархия, состоящая из трех уровней: верхний — уровень цели (выбор безопасной системы мгновенного обмена сообщениями), средний — критерии оценки (сквозное шифрование, протокол шифрования, desktop-клиент с шифрованием, шифрование голосовых звонков и ID при регистрации) и нижний — список альтернатив (в качестве альтернатив были выбраны следующие мессенджеры, популярные на современном рынке — CriptoCat, Signal, Skype, Telegram, Threema, Viber и WhatsApp).

Для формализации оценки экспертов используется специальная шкала оценок — шкала относительной важности (табл. 1). Согласно этой шкале, для расчета показателей важности на первом этапе производится постановка и формализация задачи [Саати, 1993].

Таблица 1
Table 1

Шкала относительной важности
The scale of the relative importance

Степень значимости	Определение
0	Несравнимы
1	Равная важность
3	Умеренное превосходство одного над другим
5	Существенное или сильное превосходство
7	Значительное превосходство
9	Очень сильное превосходство
2,4,6,8	Промежуточные решения между двумя соседними суждениями
Обратные величины приведенных выше чисел	Если при сравнении одного вида деятельности с другим получено одно из чисел (например, 3), то при сравнении второго вида деятельности с первым получим обратную величину (т.е. 1/3)

Все альтернативы сравниваются попарно по отношению к их влиянию на общую для них характеристику (критерий). Парные сравнения приводят к записи характеристик сравнений в виде квадратной матрицы, которая обратно симметрична, т.е. имеет свойство:

$$a_{ij} = \frac{1}{a_{ji}} \quad (1)$$

Таким образом, элементом матрицы a_{ij} является интенсивность проявления элемента иерархии i относительно элемента иерархии j, оцениваемая по шкале интенсивности. При этом при каждом попарном сравнении рассматривается ряд некоторых вопросов, например, какой из элементов важнее или имеет большее воздействие, какой из них предпочтительнее и т.д. Для каждого из критериев строится и заполняется матрица парных сравнений альтернатив (табл. 2).

Подобная модель используется и для построения матрицы попарных сравнений критериев.

Если рассматривается n факторов, то всего возможно наличие следующего числа значащих сочетаний:

$$\frac{n^2-n}{2} \quad (2)$$

Для ранжирования критериев необходимо вычисление весов. Одним из возможных методов к аппроксимации вектора весов является вычисление собственного вектора матрицы парных сравнений, равного соответствующему максимальному собственному числу. Подобные алгоритмы нахождения собственного вектора уже разработаны и подробно описаны.

Таблица 2
Table 2

Модель матрицы сравнений альтернатив по первому критерию
Matrix model comparison of alternatives for the first criterion

E2EE шифрование	CryptoCat	Signal	Skype	Telegram	Threema	Viber
CryptoCat	1					
Signal		1				
Skype			1			
Telegram				1		
Threema					1	
Viber						1

МАИ располагает встроенным критерием качества работы — индексом согласованности (ИС), определяющим степень нарушения численной (кардинальной) и транзитивной (порядковой) согласованности. Кардинальная проверка заключается в контроле за определенными числовыми характеристиками, отклонение от которых свидетельствует о наличии ошибок. То есть, суждения не должны выходить за рамки установленных этими правилами множества значений (быть отрицательными или больше единицы). Транзитивность определяет верность логики: если критерий А превосходит критерий В, а В, в свою очередь, превосходит критерий С, то при парном сравнении С не должен превосходить А, следовательно должно выполняться неравенство А > В > С. Отсутствие согласованности может быть серьезным ограничивающим фактором для исследования [Тутыгин, Коробов, 2010].

ИС вычисляется по формуле:

$$ИС = \frac{\lambda - n}{n-1}, \quad (3)$$

где λ — собственное число, n — число сравниваемых факторов (критериев). ИС сравнивается с величиной, полученной при случайном выборе количественных величин, которая трактуется как средняя. Значения средней согласованности (СС) для случайных матриц разного порядка представлены в таблице 3, где n — число факторов (табл. 3).

Таблица 3
Table 3

Средние согласованности для случайных матриц разного порядка
The average coherence for random matrices of different order

n	1	2	3	4	5	6	7	8	9	10
СС	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

Отношение ИС к СС для матриц одного порядка определяет отношение согласованности (ОС):

$$ОС = \frac{ИС}{СС} * 100 \quad (4)$$

Заключительным этапом после проверки на согласованность является принятие решения на основе полученных результатов.

В данной работе главным требованием к безопасности мессенджера, то есть одним из основополагающих критериев, является сквозное, End-To-End шифрование (E2EE), при котором ключи шифрования хранятся только на пользовательских устройствах и не отправляются для хранения на сервер. Хранение или генерация ключей промежуточным устройством создает угрозу их компрометации. Вторым немаловажным критерием выступает использование надежного протокола шифрования (Signal — единственный протокол, одобренный E2EE) [Марков и др., 2012]. Причем надежность шифрования определяется не только алгоритмом или стандартом, но и типом шифрования, например, блочное или поточное. Оставшиеся критерии являются дополнительными и не определяют степень безопасности в полной мере, как первые два.

Шифрование голосовых звонков и desktop-клиент с шифрованием несомненно являются частью безопасности мессенджера, но социологические опросы показывают, что пользователи систем мгновенного обмена сообщениями не выделяют эти функции в качестве определяющих, а функцию голосового вызова использует крайне малое количество пользователей, поэтому она внедрена не в каждом мессенджере.

Критерий идентификатора пользователя наоборот — наиболее явно отображает степень безопасности по анонимности регистрации в мессенджерах (табл. 4).

Данные чатов в CryptoCat шифруются протоколом Off-The-Record (OTR), использующим комбинацию алгоритмов AES, симметричного ключа, алгоритма Диффи-Хеллмана и хеш-функции SHA-1 (динамический обмен ключами). Немаловажным является тот факт, что в CryptoCat невозможно сохранить историю чата. Для входа и создания чата необходимо придумать и ввести его имя (conversation name), преимущество такого подхода заключается в том, что нет необходимости привязываться к определенному логину, можно всегда выбирать другой, даже при каждой новой беседе. Связь клиента с сервером в мессенджере CryptoCat защищается благодаря протоколам TLS/SSL.

Таблица 4
Table 4

Сводные данные альтернатив по выбранным критериям
Aggregated data of alternatives for the selected criterias

Мессенджер	E2EE шифрование	Протокол шифрования	Desktop клиент с шифрованием	Шифрованные голосовые звонки	ID
CryptoCat	нет	Off-The-Record (OTR)	да	нет функции	имя чата, логин
Signal	да	Signal	нет	да	т. номер
Skype	нет	AES-256	до сервера	нет	логин
Telegram	да	своя реализация Signal (MTProto)	Cutegram	нет функции	т. номер, логин
Threema	да	ECDH	HTTPS	нет функции	QR-код
Viber	да	часть Signal (Double Ratchet)	до сервера	да	т. номер
WhatsApp	да	Signal	HTTPS	да	т. номер

Мессенджер Signal компании Open Whisper Systems использует Open Source протокол (протокол Signal — модель сквозного шифрования E2EE с PFS — совершенной прямой секретностью, гарантирующей, что сессионные ключи не будут скомпрометированы при компрометации одного из долговременных ключей) [WhatsApp Encryption Overview, 2016].

Протокол MTProto, используемый в Telegram, шифрует данные до их отправки транспортным протоколом, например таким, как TCP, HTTP, UDP и т.д. (рис.).

Рис. Схема шифрования протокола MTProto
Fig. Encryption scheme of the MTProto protocol

При 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.

Thremma — безопасный мессенджер из Швейцарии с шифрованием на базе алгоритма протокола Диффи-Хеллмана на эллиптических кривых (ECDH), имеет защищенный механизм

верификации контактов (требуется при личной встрече просканировать с экрана абонента специальный QR-код) [Threema Cryptography Whitepaper, 2016]. В начале создания у мессенджера была уязвимость, которая заключалась в проблемах с шифрованием: потоковый шифр RC4 создавал потоки из байт, поддающиеся криптографии с помощью простого текста в зашифрованную последовательность, и если шифр был одинаков для двух потоков, то восстановить сообщения можно было простым сравнением шифрованных данных. Со временем разработчики приложения устранили этот недостаток.

Метод анализа иерархий позволяет обрабатывать большое количество данных и качественно анализировать их, что подтверждается в данном исследовании. МАИ представляет собой идеальный инструментарий для решения широкого круга многофакторных задач, а оценка меры противоречивости использованных данных позволяет установить степень доверия к полученному результату. Результатом расчетов является выбор альтернатив с наибольшим приоритетом. Однако, у метода есть и недостатки, а именно — использование транзитивности для качественных показателей. Отношение транзитивности хорошо работает, когда все характеристики исследуемой системы можно представить числовыми величинами. Но как только это становится невозможным, требование наличия транзитивности зачастую вступает в противоречие с логикой.

Выводы

Для проведения обоснованных численных сравнений не рекомендуется сравнивать более 7—9 элементов, что было учтено при исследовании, для оптимальной оценки было выбрано семь альтернатив. В этом случае малая погрешность в каждой относительной величине незначительно влияет на ее значение. По результатам анализа систем мгновенного обмена сообщениями при помощи МАИ были выявлены следующие четыре системы, расположенные в порядке по убыванию оценки приоритетности: Threema, Signal, CryptoCat, Telegram.

Формирование структуры модели принятия решения в методе анализа иерархий достаточно трудоемкий процесс. Однако в итоге удается получить детальное представление о том, как именно взаимодействуют факторы, влияющие на приоритеты альтернативных решений, и сами решения, что позволяет в будущем строить модели выбора, используя не только другие критерии и альтернативы, но и цели.

Список литературы
References

Threema Cryptography Whitepaper, 2016-07-05. 12.

WhatsApp Encryption Overview, april, 2016. 9.

Жукова П.Н., Насонова В.А., Ходякова Н.В. 2015. О некоторых средствах зашиты информационных систем от несанкционированного доступа. Общие и комплексные проблемы технических и прикладных наук и отраслей народного хозяйства: Проблемы правоохранительной деятельности. №2. 83-88.

Zhukova P.N., Nasonova V.A., Hodjakova N.V. 2015.O nekotoryh sredstvah zashhity informacionnyh sistem ot nesankcionirovannogo dostupa. Obshhie i kompleksnye problemy tehnicheskih i prikladnyh nauk i otraslej narodnogo hozjajstva: Problemy pravoohranitel'noj dejatel'nosti. [About some of the protection means of information systems against unauthorized access. Common and complex problems of technical and applied Sciences and branches national economy: Problems of law enforcement]. (2): 83-88. (in Russian)

Марков А.С., Цирлов В.Л., Барабанов А.В. 2012. Методы оценки несоответствия средств зашиты информации. М.: Радио и связь, 192 с.

Markov A.S., Cirlov V.L., Barabanov A.V. 2012. Metody ocenki nesootvetstvija sredstv zashhity informacii. [Assessment methods inconsistency of information security tools]. Moscow: Radio i svjaz', 192. (in Russian)

Саати Т. 1993. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 278 с.

Saati T. 1993. The decision making. The analytic hierarchy process. [The decision making. The analytic hierarchy process]. Moskow, Radio i svyaz, 278. (Saati T. 1980. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation, McGraw-Hill New York)

Тутыгин А.Г., Коробов В.Б. 2010. Преимущества и недостатки метода анализа иерархий. Известия Российского государственного педагогического университета им. А.И. Герцена. №122. 108-115.

Tutygin A.G., Korobov V.B. 2010. Preimushhestva i nedostatki metoda analiza ierarhij. Izvestija Rossijskogo gosudarstvennogo pedagogicheskogo universiteta im. A.I. Gercena [The advantages and disadvantages of the method of hierarchy analysis. Izvestia Russian state pedagogical University. A.I. Herzen]. (122). 108—115.

Фурцев Д.Г., Коваленко А.Н., Ткаченко Е.А. 2014. Об оптимизации на основе метода анализа иерархий. Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика. 1(172): 142-149.

Furcev D.G., Kovalenko A.N., Tkachenko E.A. 2014. Ob optimizacii na osnove metoda analiza ierarhij. Nauchnye vedomosti BelGU. Istorija. Politologija. Jekonomika. Informatika [About optimization based on the method of analysis of hierarchies. Scientific sheets of BelSU. Series: History. Political science. Economy. Informatics.]. 1(172): 142-149.