ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 214 (2022). С. 60–68
DOI: 10.36535/0233-6723-2022-214-60-68

УДК 512.563+004.056.55

СЦЕНАРИЙ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНОЙ СЕТИ В КАЧЕСТВЕ ИСТОЧНИКА КЛЮЧЕВОГО МАТЕРИАЛА ДЛЯ ОДНОРАЗОВОГО ШИФРОБЛОКНОТА

© 2022 г. **В. Е. МУЦЕНЕК**

Аннотация. Описан сценарий применения социальных сетей в качестве средства доставки ключевого материала для одноразового шифроблокнота. Рассмотрены технические возможности социальной сети по доставке открытого текста, возможности автоматизации захвата данных социальной сети клиентскими приложениями для последующей обработки с точки зрения относительно криптостойкости.

Ключевые слова: информационная безопасность, одноразовый шифроблокнот, криптоанализ, социальная сеть.

THE SCENARIO OF USING A SOCIAL NETWORK AS A SOURCE OF KEY MATERIAL FOR THE ONE-TIME PAD

© 2022 **V. E. MUTSENEK**

Abstract. The scenario of use of social media as a mean for delivery of key material for the one-time pad is described. Technical capabilities of social media to deliver plain text, capabilities of automatic intercept of data from social media, and matters of cryptographic strength are considered.

Keywords and phrases: information security, one-time pad, cryptoanalysis, social media.

AMS Subject Classification: 06E30, 94D10

1. Задачи исследования. Появление социальных сетей, их укрепление в роли средств распространения информации оказали значительное влияние на процессы, происходящие в обществе. Предположим, что эволюция поведенческих шаблонов человека, вызванная влиянием современных информационных технологий, могла внести изменения и в технологии скрытой передачи информации. Данная работа ставит целью поиск ответов на вопросы:

1. Как могла трансформироваться классическая система тайной связи с появлением социальных сетей.
2. Существует ли возможность использования современных технологий распространения информации в сети Интернет для создания и поддержки классических систем тайной связи.
3. Насколько безопасны с точки зрения криптоанализа предложенные за последние несколько лет схемы одноразовых шифроблокнотов (ОШБ).

2. Объект исследования. Системы тайной связи длительное время эффективно использовались для организации канала передачи информации. Во второй половине XX в. системы тайной связи активно задействовали технические и криптографические средства.

Подробная характеристика систем тайной связи, применявшихся в XX в., дана В. В. Гребенниковым в [3]. Классическая система тайной связи включает устройство набора (кодирования), передатчик и приёмник. Отмечается, что в подобных системах «наверное, ни один элемент безопасной связи агента с Центром не применялся так часто, как ОШБ» [3, с. 82]. Существует возможность пренебречь шифрованием, если факт передачи сообщения можно скрыть [3, сс. 82, 86]. В качестве одного из каналов связи упоминается «односторонняя речевая радиопередача, которая давала возможность принимать шпионские сообщения на обычный КВ радиоприемник в диапазоне 3—30 Мгц» [3, с. 83]. Развитие односторонней системы связи в этом диапазоне привело к сокращению времени передачи сообщения с 1 часа до 10 минут. Появление систем ближней агентурной связи сократило время передачи до 3 секунд. Для канала этого типа в качестве способа сокрытия упоминается зашумление радиоэфира ложными радиопередачами [3, с. 85].

Надёжность системы, по мнению Гребенникова, обеспечивается при соблюдении условий:

1. *Безопасность*: содержимое сообщения должно быть непонятным для любого, кроме получателя. ОШБ и криптоалгоритмы должны защитить сообщение от прочтения противником, даже если оно перехвачено.
2. *Персональность*: сообщение не должно быть доступным никому, кроме получателя.
3. *Неизвестность*: наличие линии и техники связи между агентом и резидентом должно быть никому не известным.
4. *Маскировка*: осуществление связи не должно отличаться от обычных действий. Для скрытого обмена информацией в интернете нужно использовать бесплатные программы, стандартные почтовые ящики, системы общего пользования и цифровые тайники [3, с.86].

Система тайной связи, как отмечает Гребенников, должна удовлетворять следующим требованиям.

1. Прекращение передачи, если один из участников связи обнаружен, поскольку нельзя давать ссылку на человека на другой стороне канала связи. Содержание сообщения является вторичным по отношению к безопасности агента.
2. Использование наилучших из имеющихся физических или электронных методов сокрытия. Система всегда должна использовать самую передовую технику, доступную в настоящее время.
3. Использование стойкого криптоалгоритма для шифрования сообщений.
4. Устройства должны быть портативными и совместимыми с различными компьютерными аппаратными платформами.
5. Преемственность предыдущих и новейших технических решений с оптимальной гибкостью, что позволяет при наличии будущих улучшений безопасности читать сообщения старых систем скрытой связи [3, с. 88, 89].

Примем перечисленные характеристики как признаковое описание классической системы тайной связи.

3. Сравнение признаковых характеристик. Между социальной сетью и радиоканалами, использовавшимися во временной односторонней и ближней агентурной системах связи, можно провести несколько параллелей. В ситуации, когда социальная сеть используется без обратной связи, создаётся симплексный канал, подобный системе временной односторонней связи. Обе среды передачи не защищены от перехвата. В обоих случаях информационное пространство можно зашумить ложными сообщениями, затруднив обнаружение. Время передачи информации по сети Интернет сравнимо с временем работы систем ближней агентурной связи. Современные бытовые вычислительные устройства могут выступать в роли передатчика и приёмника, не вызывая подозрений, позволяют обеспечить гибкость, сохраняя неизменной аппаратную часть при совершенствовании программной. Между поколениями вычислительной техники для обеспечения обратной совместимости поддерживается преемственность на уровне стандартов.

4. Условия применения. Важным с точки зрения безопасности шифрования является ответ на вопрос, можно ли применить сообщение социальной сети в качестве криптографического ключа. Очевидным предположением является то, что само сообщение ключом являться не может в силу возможности своего обнаружения. Средние длины сообщений Twitter составляют

от 15 символов для языков с иероглифической письменностью до 28-30 символов для языков с алфавитной письменностью, по утверждениям различных СМИ и самого Twitter за 2012—2018 годы. Это даёт возможность использовать сообщения в качестве исходного материала для создания ключа с помощью гаммирования с вектором инициализации, вносимым в криптосистему независимо от сообщения. От отправителя в этом случае требуется запоминание вектора инициализации.

Условие неизвестности выполнимо при использовании только бытовых устройств. Вспомогательным фактором для обеспечения неизвестности может быть использование легко запоминающегося исходного материала, чтобы не возникало необходимости вести лишние записи. Краткое сообщение Twitter, статус или краткое сообщение любой другой социальной сети по своему объёму подходит для быстрого запоминания.

Запоминаемость исходного материала может использоваться в качестве дополнительного преимущества в условиях отложенной отправки сообщения. В условиях непосредственной отправки, при наличии стабильного соединения с сетью Интернет, сбор исходного материала может осуществляться «на лету» автоматизированным способом, например через запрос `users.get` API ВКонтакте.

В условиях информационного противоборства возможно ограничение доступа к какой-либо социальной сети, а в каналах связи могут происходить отказы оборудования, профилактические и ремонтные работы, а также атаки типа «отказ в обслуживании». Независимые резервные каналы доставки исходного материала могут быть сформированы сервисами кросс-постинга, предоставляющими услуги по одновременной, синхронной, запланированной заранее публикации в несколько социальных сетей. Кросс-постинг может осуществляться и с помощью приложений, использующих API социальных сетей.

Источник исходного материала для генерации ключа должен быть таким, чтобы обращение к нему не выделялось среди постоянных привычек участника системы тайной связи. Для человека, активно интересующегося политикой, естественным может выглядеть регулярный просмотр страниц официальных политических деятелей, например, даже Президента своей страны. Для человека, увлекающегося эстрадной музыкой, естественным поведением в социальной сети является просмотр страниц любимого музыкального коллектива. Для учёного-математика не вызовет подозрений просмотр страниц с математическими головоломками или страниц-счётчиков простых чисел (например `@primesdaily` или `@primetweetbot`). Встречаются в социальных сетях и страницы, публикующие преимущественно сообщения отвлечённого характера, без привязки к актуальной новостной повестке (примеры: `@deathstarpr` — сообщения от лица PR персонала Галактической Империи из киноэпопеи «Звёздные войны», `@thetweetofgod` — высказывания от лица Бога, `@ohwonka` — сообщения от лица выдуманного персонажа Вилли Вонка, причём текст сообщений последнего преимущественно передавался с помощью изображений, вероятно, чтобы избежать индексации поисковыми роботами). Среди ботов, по длине или содержанию сообщений удовлетворяющих параметрам каналов передачи исходного материала, могут быть и боты-словари (например, `@everyword`, публиковавший по одному словарному слову в день с 2007 по 2014). Результаты исследований [2, 4, 14] позволяют утверждать, что регулярное посещение интернет-ресурсов не является чем-то необычным и поэтому может не вызывать подозрений.

Факты использования шифрования по определённым протоколам и осуществления тайной связи не должен демаскироваться обращениями к серверам арбитража (в этом случае предположения о принадлежности серверов арбитража дополнительно демаскируют связи абонентов).

5. Общая характеристика ОШБ. Можно ожидать, что для связи в подобных ситуациях стороны постараются использовать проверенный, стойкий, нетребовательный к вычислительным ресурсам алгоритм, способный эффективно работать в программном исполнении, легко воспроизводимый с помощью любых существующих интерпретаторов и сред разработки. Для поддержки такого алгоритма должно быть достаточно функций арифметико-логических устройств, составляющих элементную базу гражданской микроэлектроники. Требования к программной среде вариативны, поскольку среди мобильных устройств наблюдается широкое разнообразие операционных систем. Однако для снижения заметности системы целесообразно, чтобы вычисления

в ней могли проводиться без применения специальных программ, и задействовали вместо этого скриптовые языки программирования, интерпретаторы или электронные таблицы. Из существующих алгоритмов, удовлетворяющих этим требованиям, одноразовый блокнот является наиболее известным и распространённым.

Попытки актуализировать использование одноразового блокнота в последнее время предпринимались неоднократно. В некоторых случаях одноразовый блокнот применялся не как самостоятельная криптосистема, а как составная часть стеганографических систем [15]. Другие попытки были направлены на модификацию алгоритма Вернама с целью решения проблем распределения и повторного использования ключей [6], и на специфические применения одноразовых блокнотов (для шифрования данных облачного хранилища [8], в качестве средства защиты канала связи с БПЛА [1], в качестве схемы шифрования в квантовой криптографии [17]).

Квантовые компьютеры всё ещё остаются только экспериментальными устройствами, поэтому связанные с ними реализации одноразовых блокнотов не представляют интереса с точки зрения данной работы. Также в контексте систем тайной связи не представляют интереса реализации одноразового блокнота, в которых ключ не передаётся или стороны обмена сообщениями дефакто начинают и заканчивают обмен личной встречей (как в случае с БПЛА).

Говоря об одноразовых блокнотах, нельзя не вспомнить системы шифрования с открытым ключом, такие как EPOC-2, который в комбинации с одноразовым блокнотом был сочтён семантически безопасным, устойчивым к атакам на основе подобранного шифротекста (IND-CCA2 или NM-CCA2), и тем не менее в отношении которого было доказано существование атаки по двум побочным каналам: на основе сообщений об ошибке [12] и по времени выполнения [19]. В алгоритме EPOC-2 ключи генерируются с помощью параметра безопасности и двух простых чисел p и q.

В ходе исследования были изучены несколько алгоритмов одноразового блокнота. Все они обладали уязвимостями, большинство которых по характеру можно отнести к уязвимостям архитектуры. Рассмотрим различные схемы применения ОШБ подробнее.

6. ОШБ с арбитром ключей. Схема, представленная в работе [7], ориентирована на защиту локального устройства. Разработчики допускают использование схемы при обмене сообщениями и предлагают в этом случае распределять ключи между абонентами с применением существующих криптографических протоколов. Отличительной особенностью схемы является хэширование ключей и хранение отпечатков ключей (Key Foot Prints) в устройстве, для контроля подачи на вход шифра уже однажды использованного ключа. Способов распределения списков отпечатков ключей между абонентами системы связи не предлагается.

Развивая мысль, высказанную Бансимба и др., отметим: идея применения хэш-значений от ключей для контроля применимости может быть воплощена в виде третьей стороны обмена сообщениями, назовём её «арбитр ключей». Основная функция «арбитра ключей» — приём и публикация отпечатков ключей. Отметим, что «арбитр ключей», отпечатки которых основаны на известных функциях хэширования, может по мере развития методов криптоанализа оказаться уязвимым к атакам, направленным на поиск коллизий и прообразов. Также наличие в системе шифрования «арбитра ключей» демаскирует факт передачи сообщения, так как без обращения к арбитру с хэш-кодом в качестве аргумента операция шифрования становится неосуществима. По времени обращения к арбитру, регистрируемому средствами перехвата трафика, и событиям системного журнала устройства может быть определён диапазон хэш-значений для проведённых в окрестности события операций шифрования.

7. Стеганографическая система на основе ОШБ. Пелоси, Кесслер и Браун в [15] предложили реализацию платформы рабочей среды адаптивной стеганографической системы с применением одноразового блокнота. Разработанное ими программное решение не обеспечивает распределения ключей. Также в рекомендациях по применению обозначена необходимость использования компьютера, изолированного от сетей общего пользования и международного информационного обмена. Таким образом, данная стеганографическая система неудобна для применения в качестве системы тайной связи.

8. ОШБ на основе дополнений двоек. Вариант одноразового блокнота был предложен в [13]. Алгоритм выполняется в двоичном алфавите и включает две операции. Первый шаг состоит из сложения ASCII кодов символов открытого текста P, представленных в двоичном виде, с ключом (простым числом в двоичном алфавите) K, и вычисления второго дополнения к результату этой операции. Затем из результата первого этапа вычитается P:

$$C_i = ((P_i + K)^C + 1_2) - P_i. \tag{1}$$

Указанные операции описаны в алгоритме как выполняемые посимвольно. Таким образом, схема (1) не представляет интереса с точки зрения криптостойкости, так как в предложенном алгоритме осуществляется по сути отображение алфавита открытого текста в алфавит шифротекста. Схема также не содержит усовершенствований в части управления ключами. Использование её без модификаций нецелесообразно, так как в шифротексте сохранятся статистические зависимости, присущие языку человеческого общения. Однако если соблюсти принципы построения классического одноразового блокнота, а именно длину ключа выбрать равной длине исходного сообщения, можно обеспечить ослабление зависимости результата от исходного текста. Ключ тем не менее нельзя будет использовать повторно.

9. ОШБ с примитивной стеганографией. Группой исследователей из Universiti Sains Malaysia и The Islamia University of Bahawalpur была предложена схема одноразового блокнота, сочетающая шифрование с примитивной стеганографией. Основная цель работы заключалась в уходе от необходимости генерировать уникальный ключ каждый раз, когда выполняется новое шифрование. Схема устойчива к атаке по известному открытому тексту. Схема [6] представляет собой блочный симметричный шифр, выполняющийся в несколько этапов. Алфавитом исходного текста и шифротекста является 8-битная таблица символов. Первый этап включает формирование ключа шифрования K из набора ключей: n-байтного K_A и однобайтного K_B:

$$K = K_{A_1} \oplus K_{A_2} \oplus \ldots \oplus K_{A_n} \oplus K_B. \tag{2}$$

Исходный текст P дополняется спереди случайным вектором R, кратным длине блока:

$$M = (R\&P). \tag{3}$$

На втором этапе осуществляется блочное шифрование в режиме сцепки блоков:

$$\begin{cases} C_1 = M_i \oplus K, \\ C_{i+1} = M_i \oplus C_i \oplus K. \end{cases} \tag{4}$$

На дешифрование блоки шифротекста подаются в обратном порядке.

Предложенная схема вносит достаточный уровень диффузии. Демонстрационный пример тем не менее содержит несколько особенностей, делающих схему, используемую непосредственно в нём, уязвимой. Во-первых, длина ключа, получаемого из двух источников (как минимум один из которых является естественным генератором случайных чисел), сводится в итоге к длине блока. Длина блока в демонстрационном примере равна длине кода символа в таблице символов.

Стойкость схемы, работающей в алфавите языка человеческого общения, в данном случае будет ограничена разрядностью таблицы символов, и для 8-битного ключа составит всего 2^8. Вычисление всего текста в рассмотренном примере не требуется для проверки гипотезы о ключе, достаточно лишь заключительных блоков. Разумно предположить, что стойкость будет возрастать при увеличении разрядности таблицы символов, если не брать во внимание особенности кодирования. Например, в UTF-16 символы основной латиницы содержат нулевые байты в конце (таким образом, половина бит ключа может быть заранее известна). Ещё одна уязвимость может быть связана с ограниченностью алфавита языка человеческого общения фиксированным набором символов. В обычных сообщениях, не включающих специальные символы, алфавит существенно ограничен. Подход, уравнивающий блок символу, фактически сводит для одного блока пространство размещений с повторениями из 2^n символов к нескольким десяткам заранее известных словарных комбинаций. Поэтому ограничение длины блока одним символом в (2)—(4) нежелательно.

10. ОШБ в режиме сцепки блоков. Схемы [11, 16] используют хэш-функцию и блочный алгоритм шифрования для преобразования открытого текста A в шифротекст B. Схема [11] в демонстрационном примере опирается на SHA-1 и AES с длинами дайджеста и блока 64-бита. Схема [16] опирается соответственно на DES и MD5.

На подготовительном этапе из 64-битного ключа шифрования K с помощью функции преобразования X формируется вектор инициализации:

$$B_0 = X(K). \tag{5}$$

Вычислению каждого блока шифротекста B_i предшествует вычисление ключа K_i с помощью хэш-функции:

$$K_i = H(B_{i-1}, K), \quad B_i = E_{K_i}(A_i). \tag{6}$$

В качестве X в (5) может быть использована комбинация простых операций сдвига, замены, сложения по модулю 2. Дешифрование осуществляется поблочно от начала к концу сообщения, с подготовительными операциями (5) и (6).

Схема [11] позволяет минимизировать риски, связанные с недостаточностью длины ключа, характерные для традиционных ОШБ. В некоторых условиях схема даёт возможность для атаки на последний цикл вычислений алгоритма на основе пары открытого и зашифрованного текстов. Так, файлы формата png завершаются последовательностью байт 49 45 4E 44 AE 42 60 82. В этом случае для 64-разрядного блока взломщику становится известны B_n и A_n. Это является достаточным условием для осуществления атаки со сложностью не более чем 2^{16} (см. [5, с. 54]), в результате которой злоумышленнику может стать известен ключ K_n. Теоретические основы осуществления атак нахождения коллизий для SHA-1 были известны ещё с 2005 г. (см. [18]). Возможности реализации комбинированной атаки по нахождению K при обнаруженных B_{n-1} и K_n будут зависеть от примененных в схеме алгоритмов.

11. Многослойный ОШБ. Сложный способ многослойного шифрования по схеме одноразового блокнота предложен Бросас, Сайсон и Медина в [9]. В схеме используется случайный вектор инициализации IV, формирующий последовательность S, участвующую в преобразовании ключевого материала K в ключ первого слоя $CK1$, из которого через цепочку сдвигов получается $CK2$:

$$\begin{gathered} S_n = S_{n-1} \oplus (IV_{n+1} \oplus K_{n+1}) \bmod 256, \\ CK_n = CK_{n-1} \oplus (S_{n+1} \oplus K_{n+1}) \bmod 256, \\ \begin{cases} CK1_0 = CK1 < 1, \\ CK1_1 = CK1_0 <<< 3, \\ CK1_2 = CK1_1 <<<<< 5, \\ CK2 = CK1_2, \end{cases} \end{gathered} \tag{7}$$

где символ $<$ означает сдвиг на 1 бит влево.

Первый слой шифра [9] состоит из замены открытого текста, по таблице кодирования ДНК. Результатом является шифротекст первого слоя $CT1$. На втором слое $CT1$ подвергается операции сложению по модулю 2 с ключом $CK1$, и поступает на вход функции обратной связи. $CT3$ порождается сложением $CT2$ по модулю 2 с $CK2$. Эти операции авторы алгоритма называют «Cross over technique». Третий слой составлен из трёх итераций комбинированного шифра, в котором результат предыдущей итерации складывается по модулю с $CK2$, затем подаётся на функцию обратной связи и сдвигается на два бита влево.

Дешифрование в схеме [9] начинается с обращения трёх итераций третьего слоя, с $CT5$ и $CK2$ в качестве исходных данных, продолжается обращением операций второго слоя, и завершается обращением первого слоя.

Алгоритм [9] показал соответствие строгому лавинному критерию, однако есть особенности, недостаточно раскрытые авторами этой схемы. В частности, не ясно, с какой целью в (11) сдвиг

осуществляется двумя последовательными циклами ($CK2$ в демонстрационном примере представлен как совокупный результат сдвигов $CK1$ на 3 и 5 бит). Сдвиг в третьем слое в демонстрационном примере при вычислении CT5 выполнен на три, а не на два разряда. Схема подразумевает идентичность операции по получению $CT4$ из $CT3$ и $CK2$ операции по получению $CT3$ из $CT2$ и $CK2$, однако фактическая связь между $CK3$ и $CK4$ в демонстрационном примере не отслеживается, поскольку применение обратной связи недостаточно подробно описано: OFB на вход подаются шифротекст и ключ $CK2$, однако нет упоминаний о том, что в ней используется как вектор инициализации.

Чтобы продемонстрировать важность криптостойкой функции обратной связи в рассматриваемой схеме, примем упрощение для функции обратной связи $OFB(CT) = CT$.

Для 8-битного укороченного сообщения получим:

$$CT5_n = CT3_{(n+4) \bmod 8} \oplus CK2_{(n+2) \bmod 8} \oplus CK2_n,$$

соответственно для сообщения длиной 256 бит:

$$CT5_n = CT3_{(n+4) \bmod 256} \oplus CK2_{(n+2) \bmod 256} \oplus CK2_n.$$

Учитывая, что $CK2$ получен в результате сдвига $CK1$ на 8 разрядов, имеем

$$\begin{aligned} CT2_n &= CT1_n \oplus CK2_{(n+8) \bmod 256}, \\ CT3_n &= CT1_n \oplus CK2_{(n+8) \bmod 256} \oplus CK2_n, \\ CT5_n &= CT1_{(n+4) \bmod 256} \oplus CK2_{(n+12) \bmod 256} \oplus CK2_{(n+4) \bmod 256} \oplus CK2_{(n+2) \bmod 256} \oplus CK2_n. \end{aligned} \tag{8}$$

Напомним, что $CT1$ представляет собой результат кодирования по ДНК-таблице замен, что подразумевает отображение символов исходного текста в набор словарных конструкций длиной 8 бит. Они будут иметь те же частотные характеристики, что и символы языка человеческого общения. Согласно (8) для подобного упрощения могут существовать слабые ключи $CK2$, в которых биты повторяются с периодом 8. Тогда третий слой становится не более чем предсказуемой перестановкой результата вычисления второго слоя.

В условиях рассмотренного упрощения результат всего шифрования оказывается зависим от результата вычисления $CK2_{(n+12) \bmod 256} \oplus CK2_{(n+4) \bmod 256} \oplus CK2_{(n+2) \bmod 256} \oplus CK2_n$, и при слабом ключе $CK2$ становится либо инверсией, либо прямым отображением $CT1$ со сдвигом.

Дальнейшее развитие работы Бросас и др., выраженное в [10], так же не предоставляет гарантированно надёжного решения проблемы выбора векторов инициализации для функций обратной связи. В частности, предлагается использовать в качестве гаммы и векторов инициализации время отправки сообщения и стартовый адрес сообщения в памяти устройства. Это ведёт к появлению уязвимостей, обусловленных возможностью отслеживания времени отправки сообщения и адреса сообщения в оперативной памяти, а также связанных с особенностями выделения оперативной памяти вычислительным задачам.

Исполняемый код можно заставить размещаться по предсказуемым адресам как минимум в трёх случаях. Первый, и наиболее очевидный, это загрузка по адресам, выделяемым из адресного пространства, зарезервированного за отладчиком. Второй, предполагающий особые параметры сборки исполняемого файла или его модификацию, это манипуляции с базовым адресом образа исполняемого файла и таблицами релокации (вплоть до отключения их использования). Третий, предполагающий использование самомодифицирующегося вредоносного программного обеспечения, это манипуляция доступным адресным пространством (принудительное ограничение доступного адресного пространство через размещение в памяти недублируемых страниц, порождаемых множеством вредоносных вычислительных задач). В любом из трёх перечисленных условий адрес в области данных, где может храниться шифруемое сообщение, становится предсказуемым.

12. Выводы. Таким образом, можно утверждать, что существует техническая возможность использования информационного пространства социальных сетей в качестве среды распространения информации, являющейся исходным материалом для криптографических ключей системы тайной связи. Ответ на вопрос, используется ли эта техническая возможность, требует накопления и анализа дополнительной информации и лежит за рамками данного исследования. Организация системы тайной связи с помощью шифроблокнота, элементы которого распространяются в зашумленном информационном пространстве социальных сетей, не требует наличия специальных устройств. Поведение абонента подобной системы в повседневном режиме укладывается в шаблоны поведения пользователей социальных сетей. Поведение в процессе подготовки к отправке сообщения сформирует цепочку событий, часть которой может быть зафиксирована подсистемами регистрации событий компьютерных систем.

Среди рассмотренных схем шифрования с применением технологии одноразовых блокнотов, наиболее применимы для систем тайной связи с передачей элементов исходного материала через социальную сеть алгоритмы [11] и [9, 10]. Из них только [9, 10] не требует твёрдых навыков программирования, достаточно стоек, может быть реализован на интерпретаторах и в приложениях электронных таблиц. Однако [9, 10] недостаточно качественно описан. Помимо этого стоит отметить, что все рассмотренные алгоритмы обладали уязвимостями, большинство которых по характеру можно отнести к уязвимостям архитектуры.

СПИСОК ЛИТЕРАТУРЫ

1. *Авдонин И. А., Будько М. Б., Грозов В. А.* Организация защиты данных, передаваемых между беспилотным летательным аппаратом и наземной станцией управления, на основе шифра Вернама// Науч.-техн. вестн. информ. технол. мех. опт. — 2016. — № 5. — С. 850–855.
2. *Артамошкин М.* Отбор признаков пользователя социальной сети для построения модели машинного обучения. `https://blog.zverit.com/`.
3. *Гребенников В. В.* Американская криптология. История спецсвязи. — М.: Литрес: Самиздат, 2019.
4. *Дужникова А. С.* Социальные сети: современные тенденции и типы пользования// Мониторинг общественного мнения. — 2010. — № 5 (99). — С. 238–251.
5. *Жуков К. Д.* Обзор атак на AES-128: к пятнадцатилетию стандарта AES// Прикл. дискр. мат. — 2017. — № 35. — С. 48–62.
6. *Abiodun E. O., Aman J., Oludare I. A., Humaira A.* An enhanced practical difficulty of one-time pad algorithm resolving the key management and distribution problem// in: Lect. Notes Eng. Comput. Sci./ Proc. Int. Multiconf. of Engineers and Computer Scientists (Hong Kong, March 14–16, 2018), 2018. — P. 409–415.
7. *Bansimba G. R., Babindamana R. F., Peter A. G.* A new approach in one time pad key management// Res. J. Math. Comput. Sci. — 2019. — *3*, № 17. — P. 1–8.
8. *Blackledge J. et al.* Secrecy and randomness: encoding cloud data locally using a one-time pad// Int. J. Adv. Security. — 2017. — *10*, № 3–4. — P. 167–181.
9. *Brosas D. G., Sison A. M., Medina R. P.* Strengthening the Vernam cipher algorithm using multilevel encryption techniques// Int. J. Sci. Technol. Res. — 2019. — *8*, № 10. — P. 601–606.
10. *Brosas D. G., Sison A. M., Medina R. P., Hernandez A.* Analysis of the randomness performance of the proposed stream cipher based cryptographic algorithm// 11th IEEE Control and System Graduate Research Colloquium (Shah Alam, Malaysia, 2020), 2020. — P. 76–81.
11. *Chandrakar S., Tiwari S., Shree Jain B.* An innovative approach for implementation of one-time pads// Int. J. Comput. Appl. — 2014. — *89*, № 13. — P. 35–37.
12. *Dent A. W.* Implementation attack against EPOC-2 public-key cryptosystem// Electr. Lett. — 2002. — № 38. — P. 412–413.
13. *Devipriya M., Sasikala G.* A new technique for one time pad security scheme with complement method// Int. J. Adv. Res. Comput. Sci. Software Eng. — 2015. — *5*, № 6. — P. 220–223.
14. *Limaye S., Thadathil R.*. Influence of social media on behavior patterns// Proc. Natl. Conf. on Research In Information Technology And Management (Bangalore, 2016), 2016. — P. 1–4.
15. *Pelosi M. J., Kessler G., Brown M. S. S.* One-time pad encryption steganography system// Proc. Conf. "Annual ADFSL Conference on Digital Forensics, Security and Law" (Daytona Beach, Florida, 2016), 2016. — P. 131–154.

16. *Tang S., Liu F.* A one-time pad encryption algorithm based on one-way hash and conventional block cipher// Proc. 2 Int. Conf. on Consumer Electronics, Communications and Networks, 2012. — P. 72–74.
17. *Upadhyay G., Nene M. J.* One time pad generation using quantum superposition states// Proc. IEEE Int. Conf. on Recent Trends in Electronics, Information, and Communication Technology (Bangalore, 2016), 2016. — P. 1882–1886.
18. *Wang X., Yin Y. L., Yu H.* Finding collisions in the full SHA-1// Adv. Cryptology. — 2005. — *3621*. — P. 17–36.
19. *Zhou Y., Feng D.* Side-channel attacks: ten years after its publication and the impacts on cryptographic module security testing/ Cryptology ePrint Archive, Report 2005/388. `https://ia.cr/2005/388`.

Муценек Витус Евгеньевич
Иркутский государственный университет
E-mail: `comsecsurvey@gmail.com`