DOI: 10.25728/iccss.2022.91.86.030

Синюк А.Д., Тарасов А.А.

Принципы открытого сетевого многоключевого согласования

Аннотация: Одной из сложных организационно-технических задач обеспечения информационной безопасности функционирования закрытых сетей связи, использующих криптографические методы, является оперативное восстановление скомпрометированного нарушителем общего ключа. Решение возможно на основе формирования сетевого ключа по открытым каналам связи. Частые повторные компрометации сетевого ключа вызывают существенное увеличение времени его восстановления. Предлагаются принципы открытого сетевого многоключевого согласования, определяющие условия построения конструктивных протоколов формирования увеличенной криптосвязности корреспондентов сети связи, которая обеспечит оперативное восстановление сетевого ключа.

Ключевые слова: закрытая сеть связи, сетевой ключ, групповой ключ, парные ключи, нарушитель, протокол открытого сетевого многоключевого согласования

Обмен информацией между корреспондентами сети связи (СС), закрытый на сетевом ключе, имеет ряд преимуществ. Однако компрометация сетевого ключа нарушителем влечет за собой полную потерю криптографической связности одновременно всех корреспондентов закрытой СС [1].

Доставка нового сетевого ключа по защищенному каналу связи не всегда представляется возможной, целесообразной и требует достаточно больших организационных, материальных и временных затрат [1, 2]. Альтернативой служат методы формирования сетевого ключа по открытым каналам связи [3]. Проблема восстановления сетевой криптосвязности усугубляется в условиях частых повторных компрометаций уже вновь восстановленных сетевых ключей, когда закрытый информационный обмен корреспондентов в сети связи останавливается вовсе [1, 2].

Актуализируется поиск путей построения конструктивных протоколов формирования сетевого ключа по открытым каналам связи, для которых время ключевого согласования существенно минимизируется. Решение возможно на основе подхода открытого сетевого многоключевого согласования [4], когда в ходе реализации протокола одновременно формируются вместе с сетевым (групповым) ключом еще несколько ключей между различными парами корреспондентов. Это позволит после выявления компрометации сетевого ключа быстро его восстановить с использованием оставшихся нескомпрометированных парных криптосвязностей (ключей) корреспондентов сети связи [4]. Разрабатываются принципы открытого сетевого многоключевого согласования, позволяющие синтезировать искомые протоколы.

Реализация протокола открытого сетевого многоключевого согласования (ПОСМС) в СС включающей трех корреспондентов *A, C* и *B*, возможна путем осуществления обмена данными конечной длины между ними по каналам связи (КС), доступным нарушителю (НРЛ) *E*. При этом требуется обеспечить оперативное и одновременное формирование как сетевого ключа (СК) так и парных ключей (ПК) с требуемыми вероятностью попарного совпадения СК и ПК, достоверностью, вероятностью совпадения с соответствующим ключом НРЛ.

Обмен информации в СС описывается моделью передачи информации (МПИ), в которой каналы описываются моделями двоичных симметричных КС без памяти (ДСК) [5]. Канал 1 — КС от корреспондента *A* к корреспонденту *B* с вероятностью ошибки p_y, а Канал 2 —от корреспондента *A* к корреспонденту *C* – p_m. Совокупность Канала 1 (КС1) и Канала 2 (КС2) описывается моделью двоичного широковещательного канала без памяти (ДШК) [5]. Передача сигналов по ДШК определяется составляющими КС1 (СК1) и КС2 (СК2) с алфавитами входным *X,* выходными *Y* и *M*. На вход ДШК двоичный источник информации без памяти (ДИИБП) с равномерным выходом [6] корреспондент *A* подает в виде последовательности $\bar{x}\in X^N$, где X^N – декартова *N*-я степень *X* [5, 6], корреспондент *B* принимает на выходе КС1 последовательность $\bar{y}\in Y^N$ и корреспондент *C* на выходе КС2 - $\bar{m}\in M^N$.

Каналом перехвата (КП) НРЛ определяется КС от корреспондента *A* к *E*, который описывается моделью ДСК с

вероятностью p_w с входным алфавитом X и выходным алфавитом Z. E принимает на выходе КП последовательность $\bar{z} \in Z^N$.

В МПИ имеются каналы без ошибок (p=0), которые позволяют сформировать между корреспондентами группу каналов обратной связи (КОС) [5]: первый КОС от корреспондента A к корреспонденту B (КОС-1), второй КОС от корреспондента B к корреспонденту A (КОС-2), третий КОС от корреспондента A к корреспонденту C (КОС-3), четвертый канал КОС от корреспондента C к корреспонденту A (КОС-4), 5-й КОС от корреспондента B к корреспонденту C (КОС-5), 6-й КОС от корреспондента C к корреспонденту B (КОС-6). НРЛ контролирует каждый КОС соответствующим идеальным КП обратной связи (КПОС).

Принципы одновременного формирования СК и двух ПК в МПИ заключаются в реализации задач четырех последовательно выполняемых этапов. Первый определяет задачу создания условий, при которых из исходных ДШК и КП, создаются «виртуальные» ДШК и КП, для которых качество первого улучшается по отношению к качеству второго (генерирование начальных данных (НД) корреспондента A последовательности символов $\bar{x}$ и получение НД корреспондентами B и C: последовательностей $\bar{y}$ и $\bar{m}$ на выходах СК1 и СК 2).

Второй этап – формирование начальных данных для одновременного синтеза сетевого и парных ключей: последовательности $\bar{x}$, $\bar{y}$ и $\bar{m}$ выбираются корреспондентами как исходный материал для одновременного формирования ключей. Наличие ошибок в КС1 и КС2 позволяет создать условия для одновременного формирования различающихся СК и ПК [4].

Третий этап предназначен для обеспечения формирования ключей с высокой достоверностью, которая достигается устранением ошибок передачи НД. Для формирования СК исправление производится в НД корреспондентов B и C относительно НД корреспондента A на основе использования дополнительной информации (ДИ). Она передается от A к B и C по КОС. В результате корреспонденты формируют ключевые последовательности (КлП) для формирования СК. Подобным образом для формирования ПК между A и B коррекция производится в НД корреспондента A относительно НД корреспондента B на основе использования ДИ [7]. Она передается от B к A по КОС. В

результате корреспонденты *A* и *B* формируют КлП для формирования ПК. Одновременно для формирования ПК между *A* и *C* исправление производится в НД корреспондента *A* относительно НД корреспондента *C* на основе использования ДИ. Она передается от *C* к *A* по КОС. В результате корреспонденты *A* и *C* формируют КлП для формирования ПК.

Предполагается, что НРЛ перехватывает всю информацию, передаваемую по КПОС и использует для устранения ошибок в НД нарушителя (НДН).

Четвертый этап предназначен для обеспечения формирования ключей с малой вероятностью совпадения с соответствующим ключом НРЛ *E* путем сжатия соответствующих КлП [3].

Предполагается, что модель пассивного НРЛ *E* [3] описывается условиями, когда в ходе реализации первого этапа нарушитель получает по КП НДН $\bar{z}$, а для последующих этапов реализации протокола НРЛ знает полное описание порядка действий корреспондентов и обработки доступной ему информации.

Подводя итог, отметим, что в работе предлагаются принципы открытого сетевого многоключевого согласования, которые позволяют создать условия при реализации в ПОСМС для одновременного формирования различающихся СК и ПК, отвечающим требованиям достоверности и безопасности. Это существенно увеличивает криптосвязность корреспондентов СС и создает условия для быстрого восстановления закрытого информационного обмена в СС в случае компрометации СК (ПК) НРЛ.

Литература:

1. *Menezes A.J., Oorschot P.C., Vanstone S.A.* Handbook of applied cryptography. – CRC Press, N.Y., 1996. – 780 p.

2. *Фергюсон Нильс, Шнайер Брюс.* Практическая криптография: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 424 с.

3. *Синюк А.Д., Остроумов О.А.* Протокол открытого формирования трехстороннего ключа // Наукоемкие технологии в космических исследованиях Земли. – 2014. – Т. 6. № 2. – С. 48-52.

4. *Синюк А.Д., Тарасов А.А.* Информационные базисы открытого сетевого многоключевого согласования // Известия

Института инженерной физики. – 2022. – № 1 (63). – С. 36-42.
5. *Bernard Sklar*. Digital Communications: Fundamentals and Applications. – University of California. Los Angeles, 2007. – 1104 p.
6. *Вентцель Е.С.* Теория вероятностей: Учеб. для вузов. – 9-е изд. стер. – М.: Издательский центр «Академия», 2003. – 576 с.
7. *Берлекэмп Э.* Алгебраическая теория кодирования. – М.: Мир, 1971. – 139 с.

DOI: 10.25728/iccss.2022.68.92.031

Чеканов И.Р., Краснов А.Е.

Анализ семантических элементов базы данных экспертной системы для работы с законодательными и нормативными документами в области информационной безопасности

Аннотация: Текущее положение и острая необходимость развития области информационной безопасности, а также регламентирующих данную сферу документов отражают повышенную актуальность для любой организации и в особенности объектов критических информационных инфраструктур, в обеспечении полного понимания и ориентирования в обширном объеме нормативной базы, необходимой для ведения бизнес-процессов руководителю предприятия. Такая ситуация подчеркивает наличие спроса на использование особой экспертной системы, способной структурным образом предоставить топ-менеджеру сведения рассматриваемой области, в соответствии с поставленным им запросом, помочь в принятии управленческого решения. Важной задачей данной работы является анализ подготовленной базы данных, состоящей из выбранных нормативных и законодательных документов, имеющих наибольшую ценность в области информационной безопасности для организаций и выделение наиболее важных, примечательных закономерных особенностей и свойств, способных помочь в разработке экспертной системы