Алексей Ю. Нестеренко[1], Александр М. Семенов[2]
*Национальный исследовательский университет «Высшая школа экономики»,*
*Московский институт электроники и математики им. А.Н. Тихонова (МИЭМ НИУ ВШЭ),*
*ул. Таллинская, 34, Москва, 123458, Россия*
*[1]e-mail: anesterenko@hse.ru, https://orcid.org/0000-0002-9105-8798*
*[2]e-mail: amsemenov@hse.ru, https://orcid.org/0000-0003-3251-0534*

# КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ КОНТРОЛЬНЫХ И ИЗМЕРИТЕЛЬНЫХ УСТРОЙСТВ*

*DOI: http://dx.doi.org/10.26583/bit.2020.4.01*

*Аннотация.* В работе описываются ключевые особенности криптографического протокола, обеспечивающего защищенное взаимодействие контрольных и измерительных устройств. Описывается иерархическая структура, лежащая в основе данного протокола, и связи между транспортным и сеансовым уровнями модели ISO, к которой привязаны различные этапы обработки сообщений. Безопасность данного протокола, основана на применении стандартизированных отечественных криптографических алгоритмов и механизмов, которые позволяют обеспечить аутентификацию и целостность передаваемых данных. Протокол поддерживает различные варианты установления соединения, в зависимости от используемого метода аутентификации и технических возможностей устройств. Протокол разработан в соответствии с рекомендациями национальной системы стандартизации Российской Федерации по принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, оформлен в виде рекомендаций по стандартизации в 2020 г. В работе сформулирован ряд определенных свойств безопасности, идентичных задачам, которые ставит перед собой нарушитель при попытке компрометации работы протокола и необходимых для обоснования криптографической стойкости рассматриваемых механизмов. Показана выполнимость рассмотренных свойств безопасности, основанная на различных механизмах, заложенных в структурные элементы и логику работы протокола, и на сложности компрометации стандартизированных отечественных криптографических решений.

*Ключевые слова: криптографические протоколы, защищенное взаимодействие, свойства безопасности.*

*Для цитирования: НЕСТЕРЕНКО, Алексей Ю.; СЕМЕНОВ, Александр М. КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ КОНТРОЛЬНЫХ И ИЗМЕРИТЕЛЬНЫХ УСТРОЙСТВ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 7–16, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1301>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.01.*

***Благодарности.** Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 19-37-90155.*

Alexey Yu. Nesterenko[1], Alexander M. Semenov[2]
*National Research University «Higher school of economics»,*
*Tikhonov Moscow Institute of Electronics and Mathematics (MIEMNRU HSE),*
*Tallinskaya str., 34, 123458, Moscow, Russia*
*[1]e-mail: anesterenko@hse.ru, https://orcid.org/0000-0002-9105-8798*
*[2]e-mail: amsemenov@hse.ru, https://orcid.org/0000-0003-3251-0534*

## Cryptographic mechanisms for secure interaction of control and measuring devices*

*DOI: http://dx.doi.org/10.26583/bit.2020.4.01*

*Abstract.* The paper describes the key features of the cryptographic protocol providing secure interaction between control and measuring devices. The hierarchical structure underlying this protocol and the

relationship between the transport and session levels of the ISO model, to which different stages of message processing are linked are described. The security of the protocol is based on the use of the standardized domestic cryptographic algorithms and mechanisms that ensure the authentication and integrity of transferred data. The protocol supports different options for establishing a connection, depending on used authentication method and technical capabilities of the devices. The protocol was developed in accordance with the recommendations of the national system of standardization of the Russian Federation on the principles of development and modernization of encryption (cryptographic) means of information protection, and is designed as recommendations on standardization in 2020. In this paper a number of the certain properties of safety identical to tasks which are put by the infringer at attempt of compromise of work of the protocol and necessary for substantiation of cryptographic stability of considered mechanisms are formulated. Feasibility of the considered properties of safety, based on various mechanisms embedded in structural elements and logic of the protocol, and on complexity of compromise of the standardized domestic cryptographic solutions is shown.

*Keywords: cryptographic protocols, secure communication, security features.*

*For citation: YURIEVICH, Alexey N.; MIKHAILOVICH, Aleksandr S. Cryptographic mechanisms for secure interaction of control and measuring devices. IT Security (Russia), [S.l.], v. 27, n. 4, p. 7–16, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1301>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.01.*

***Acknowledgement.** The reported study was funded by RFBR, project number 19-37-90155.*

## Введение

Современные контрольные и измерительные устройства представляют собой большой класс технических устройств, построенных на основе микроконтроллеров с различной архитектурой. При объединении таких устройств в большие гетерогенные сети, существующие различия в технических характеристиках приводят к необходимости использовать для связи каналы, различающиеся как по своим свойствам, так и по среде распространения информации. Криптографические механизмы, используемые для обеспечения защищенного взаимодействия контрольных и измерительных устройств, не должны зависеть от физического уровня передачи информации и, в частности, от наличия или отсутствия свойства гарантированной доставки сообщений.

Другой важной особенностью взаимодействия контрольных и измерительных устройств является необходимость поддержки максимально возможного числа криптографических механизмов аутентификации участников взаимодействия, основанных как на использовании предварительно распределенной ключевой информации, так и на применении инфраструктуры сертификатов открытых ключей.

Первый механизм аутентификации применим в классе устройств, срок жизни которых невелик, а уникальная ключевая информация может быть помещена в устройство на этапе его производства. Второй механизм предпочтителен для большего класса устройств, чей срок эксплуатации превышает время действия ключевой информации, или устройств, целью которых является предоставление услуги доступа к защищенному взаимодействию различным физическим лицам (например, кассовые аппараты, терминалы удаленного доступа). При этом наличие единого криптографического механизма взаимодействия позволит объединять в сети устройства независимо от используемого ими механизма аутентификации [1].

В работе рассматривается разработанный авторами механизм взаимодействия, обеспечивающий оба механизма аутентификации. Данный механизм утвержден в качестве рекомендаций по стандартизации Р 1323565.1.028-2019.

## 1. Криптографические механизмы взаимодействия

Авторами был рассмотрен ряд существующих международных и отечественных решений с целью их адаптации под перечисленные выше задачи, в частности, рекомендации по протоколуTLS 1.2(Р 1323565.1.020-2018), и протоколу CRISP(МР 26.4.001-2019). При проектировании рассматриваемого протокола был принят во внимание опыт отечественных и зарубежных исследователей по анализу криптографических протоколов [2–6], схожих по функциональному назначению. В результате была выбрана двухуровневая модель организации защищенного взаимодействия:

- на нижнем уровне реализуется транспортный протокол – протокол отправки/получения сообщений, содержащих как открытую, так и зашифрованную части, а также имитовставку, позволяющую обеспечивать целостность передаваемых данных. При этом открытая информация используется как для формирования используемой при шифровании синхропосылки, так и для возможности реализации механизмов упорядочивания и защиты от повторов при приеме сообщений. Примером такого протокола может служить протокол ESP. Однако его прямое копирование, в данном случае, невозможно как в силу жесткой привязки к IP протоколу, так и в силу необходимости поддержки используемого в IPSec механизма security association. Протокол транспортного уровня использует криптографические механизмы, но не контролирует вопросы выработки ключевой информации;
- уровнем выше располагается сеансовый протокол, основная задача которого заключается в реализации механизмов аутентификации участников протокола, механизмов выработки и согласования смены ключевой информации. Сеансовый протокол рассматривает нижележащий транспортный протокол как криптографический туннель, через который передается информация, поступающая с прикладного уровня.

Приведенная модель позволяет отделить криптографические вопросы – вопросы аутентификации участников протокола и выработки ключевой информации, от механизмов передачи зашифрованной информации по каналам связи. Один и тот же механизм выработки ключевой информации может быть реализован как для каналов с гарантированной доставкой сообщений, так и без нее. При этом обоснование криптографической стойкости криптографических механизмов сеансового уровня не зависит от используемого транспортного протокола. Выбор криптографических алгоритмов, используемых для обеспечения защищенного взаимодействия, основывался на принципах максимального использования отечественных стандартизированных криптографических решений, в частности:

- для шифрования информации допускается использование только алгоритмов блочного шифрования, регламентируемых ГОСТ Р 34.12-2015;
- режим шифрования информации и алгоритм выработки имитовставки регламентируется ГОСТ Р 34.13-2015 и рекомендациями Р 1323565.1.026–2019;
- для аутентификации участников защищенного взаимодействия рекомендуется криптографический механизм, позволяющий связывать вместе уникальные идентификаторы и ключи аутентификации устройств;
- для аутентификации участников защищенного взаимодействия также рекомендуется применение инфраструктуры сертификатов открытых ключей; при этом обеспечивается поддержка инфраструктуры, регламентируемой Федеральным законом от 06.04.2011 № 63–ФЗ «Об электронной подписи»; алгоритмы выработки и проверки электронной подписи регламентируются ГОСТ Р 34.10-2012;

- в основу протокола выработки ключей положена схема «Эхинацея» [7], регламентируемая рекомендациями по стандартизации Р 1323565.1.004-2017;
- в качестве алгоритма выработки производной ключевой информации выбрана функция, описываемая рекомендациями по стандартизации Р 1323565.1.022-2018;
- в качестве алгоритмов выработки производных ключей шифрования и имитовставки выбраны алгоритмы, регламентируемые рекомендациями по стандартизации Р 1323565.1.017-2018;

Использование существующих и обоснованных решений позволило провести исследование криптографических механизмов защищенного взаимодействия контрольных и измерительных устройств с учетом полученных ранее результатов анализа.

## 2. Схемы работы протокола

Процесс защищенного взаимодействия начинается с установления соединения и выполнения протокола выработки ключей. Данный протокол предназначен для генерации общей для клиента и сервера ключевой информации, которая будет использована для выработки сеансовых ключей связи. Протокол выработки ключей реализуется в группе точек эллиптической кривой [8, 9].

Спецификация протокола, см. рекомендации по стандартизации Р 1323565.1.028-2019, описывает общую универсальную конструкцию установления соединения. На практике допускается использование одной из трех указанных в Р 1323565.1.028-2019 схем взаимодействия, являющиеся частными случаями общей конструкции.

Схема A1 описывает процедуру взаимной аутентификацией на основе предварительно распределенного ключа PSK и предназначена для контрольных и измерительных устройств, для которых уникальная ключевая информация может быть выработана на этапе их производства (рис. 1).

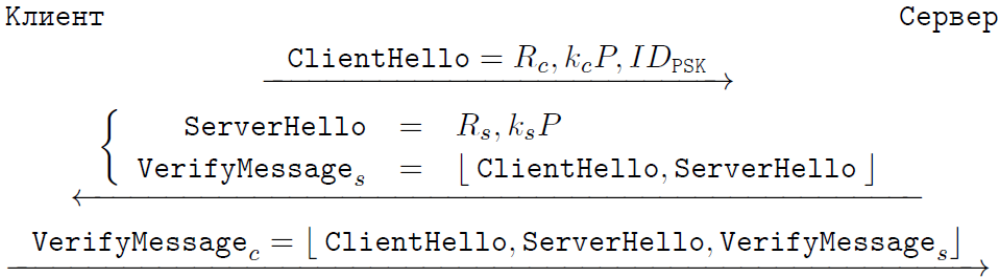


*Рис. 1. Схема аутентификации на основе предварительно распределенного ключа. Сеансовый уровень*
*(Fig. 1. Authentication scheme based on pre-shared key. Session layer)*

На сеансовом уровне сообщения рассматриваются как сериализованные представления вводимых спецификацией структур данных. Данные сообщения передаются в ходе выполнения протокола в незашифрованном виде и без имитовставок, подтверждающих целостность передаваемых сообщений. При анализе протокола мы считаем, что сеансовый уровень реализуется в «идеальном» канале связи – канале, не допускающем изменение и навязывание передаваемой информации. Транспортный уровень реализуется в «реальном» канале связи, в котором нарушитель моделируется в рамках модели Долева-Яо [10]. Такой канал требует реализации мер защиты от нарушения конфиденциальности и целостности передаваемой информации. Шифрование

передаваемых сообщений и вычисление для них имитовставки производится на транспортном уровне защищенного взаимодействия (рис. 2).


*Рис. 2. Схема аутентификации на основе предварительно распределенного ключа. Транспортный уровень*
*(Fig. 2. Authentication scheme based on pre-shared key. Transport layer)*

Другой схемой, определенной спецификацией протокола, является схема A2, регламентирующая процедуру с аутентификацией на основе ключа проверки электронной подписи (рис. 3). Для аутентификации используются ключи электронной подписи и ключи проверки электронной подписи, сертификаты которых не известны абонентам до начала выполнения протокола.

Рассматриваемая схема A2 применима для класса устройств, целью которых является предоставление услуги доступа к защищенному взаимодействию различным физическим лицам – обладателям пары асимметричных ключей аутентификации. При этом в качестве ключей аутентификации выступают ключ электронной подписи и ключ проверки электронной подписи.

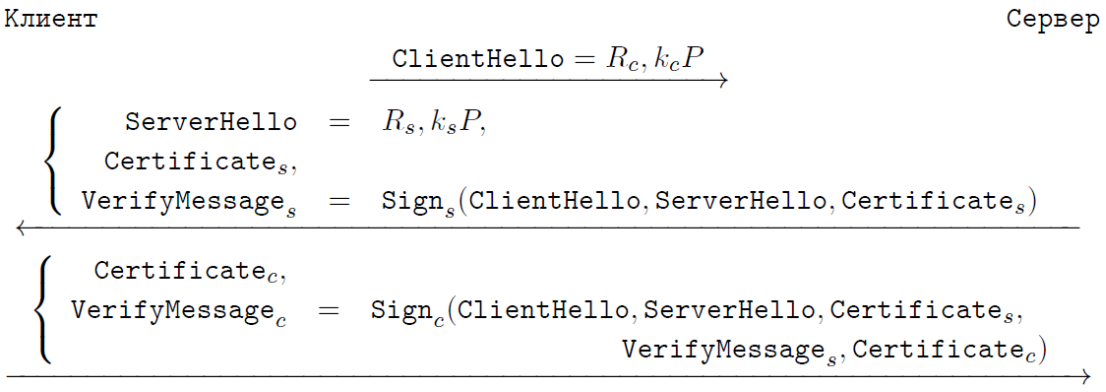


*Рис. 3. Схема аутентификации на основе ключа проверки электронной подписи. Сеансовый уровень*
*(Fig. 3. Authentication scheme based on digital signature. Session level)*

При этом, шифрование и вычисление имитовставки производится на транспортном уровне защищенного взаимодействия (рис. 4).

Спецификация предусматривает еще один вариант схемы, регламентирующий процедуру аутентификации на основе ключа проверки электронной подписи. В схеме A3 для аутентификации используются ключи электронной подписи и ключи проверки электронной подписи, сертификаты которых известны абонентам до начала выполнения

протокола. При использовании данной схемы взаимодействия стороны обмениваются не сертификатами, а информацией об используемом сертификатами ключа проверки электронной подписи, которые предварительно распределены между сторонами. В остальном взаимодействие происходит аналогично схеме А2.


*Рис. 4. Схема аутентификации на основе ключа проверки электронной подписи. Транспортный уровень*
*(Fig. 4. Authentication scheme based on digital signature. Transport layer)*

## 3. Цели нарушителя и свойства безопасности

Под целью нарушителя будем подразумевать понятие компрометации защищенного взаимодействия, заключающееся в:

- нарушении конфиденциальности;
- подделке и/или навязывании передаваемой информации;
- нарушении аутентификации участвующих во взаимодействии сторон.

При анализе защищенного взаимодействия невозможность компрометации обеспечивается выполнением ряда «свойств безопасности», комплексное выполнение которых позволяет обеспечить защиту от достижения нарушителем указанных целей.

В настоящей работе рассматривается набор свойств безопасности, разработанный международным сообществом IETF [11, 12], дополненных рядом свойств, возникших в ходе проведенного исследования. Аналогичный подход к рассмотрению свойств безопасности использован в работах [13–17]. Кратко рассмотрим указанный набор свойств.

***Формирование уникальных ключей.*** Уникальные сеансовые ключи формируются для каждого сеанса связи. Это достигается за счет использования варианта схемы Диффи-Хеллмана [18], в ходе которой вырабатывается общая случайная точка эллиптической кривой $Q = k_c k_s P$ с использованием программного или физического датчика для генерации случайных чисел $k_c$ и $k_s$.

***Стойкость при компрометации сеансовых ключей.*** Для нарушения рассматриваемого свойства с помощью теоретико-вероятностных и/или статистических методов анализа должна использоваться зависимость между ключами из различных сеансов связи. Поскольку для выработки сеансовых ключей из общей точки эллиптической кривой $Q$используется криптографическая функция HMAC [19], описанная в рекомендациях по стандартизации Р 50.1.113-2016, то можно сделать вывод, что сложность восстановления сеансовых ключей из одного сеанса по известным ключам из другого сеанса не меньше, чем сложность обращения функции HMAC.

***Защита от чтения вперед/назад.*** Выполнение данного свойства подразумевает, что сеансовый ключ, генерируемый с использованием долговременных ключей, не будет

скомпрометирован, в случае компрометации одного или нескольких долговременных ключей.

В качестве долговременного ключа в схеме A1 используется предварительно распределенный ключ аутентификации PSK. Данный ключ используется в ключевой развертке при формировании ключевой информации, используемой для получения производных ключей шифрования и имитозащиты. Также при формировании ключевой информации используется общая точка эллиптической кривой $Q$. Таким образом, знание ключа PSK недостаточно для определения производных ключей, а сложность компрометации ключей не менее, чем сложность решения задачи дискретного логарифмирования в группе точек эллиптических кривых.

Для остальных схем под долговременными ключами понимаются секретные ключи цифровой подписи, которые напрямую не участвуют в генерации сеансовых ключей шифрования.

***Подтверждение ключа.*** Подтверждение ключей шифрования и имитозащиты происходит за счет использования сообщения VerifyMessage, которое отправляется в зашифрованном виде. Последовательные расшифрование и проверка имитовставки позволяют другому абоненту подтвердить факта наличия обоих ключей у другого абонента. Более того, косвенно подтверждаются корректность использованной ключевой информации и целостность сеанса связи, так как при формировании сеансовых ключей используются хэш-коды всей переданной при установлении соединения информации.

***Аутентификация абонентов.*** Способ аутентификации абонентов зависит от выбранной схемы работы протокола. Аутентификация осуществляется на основе сертификатов открытого ключа или предварительно распределенного ключа PSK путем отправки случайных данных и проверки имитовставки или электронной подписи от отправленных данных.

***Аутентификация сообщения.*** Аутентификация источника данных для схемы A1 основана на выполнении свойства аутентификации пользователя и свойства подтверждения ключа для ключа PSK. Выполнение данных свойств позволяет идентифицировать автора сообщения по факту обладания секретным ключом PSK, а также закрепить авторство передаваемых сообщений за счет использования имитовставок и выполнения свойства подтверждения и аутентификации для ключей шифрования.
Аутентификация источника данных для остальных схем основана на выполнении свойств аутентификации пользователя и использовании электронных подписей, которые позволяют явно определить автора сообщения.

***Свойство защищенной возможности договориться о параметрах безопасности***. Выполнение данного свойства обеспечивается тем, что передаваемые сообщения между абонентами сообщения VerifyMessage содержат криптографические контрольные суммы, содержащие информацию о переданных параметрах. Кроме того, выполнение свойства подтверждения ключей для всех рассмотренных схем косвенно позволяет убедиться в целостности передаваемых сообщений и параметров безопасности.

***Свойство аутентификации ключа.*** В ходе выполнения протокола осуществляется привязка ключей к текущему сеансу связи и сформированным в рамках соединения сообщениям. Тогда выполнение свойства аутентификации ключа следует из выполнения совокупности свойств аутентификации и подтверждения ключа.

Если одновременно выполнено свойство аутентификации и свойство подтверждения ключа, то один абонент получает подтверждение того, что другой абонент явно идентифицирован и обладает корректно сформированными ключами. Выполнение свойства защиты от чтения вперед/назад и свойства защищенной возможности

договориться о параметрах безопасности, в совокупности с выполнением свойств аутентификации и подтверждения ключа, гарантирует, что в текущем сеансе ни один другой абонент, выбранный заранее, не может получить доступ ни к одному формируемому сеансовому ключу.

***Защита от навязывания ключевых значений.*** Выполнение данного свойства следует из выполнения свойства аутентификации ключа и свойства защищенной возможности договориться о параметрах безопасности.

***Анонимность идентификаторов.*** Пассивный нарушитель, прослушивающий канал связи, не имеет возможности определить идентификаторы пользователей, поскольку идентификаторы либо передаются в зашифрованном виде, либо используются неявно. В последнем случае они считаются известными участникам до начала процесса установления соединения.

В случае активного нарушителя данное свойство выполняется только для идентификатора клиента. Действительно, злоумышленник может инициировать сессию протокола, выдавая себя за клиента, и, получив ответ от сервера, определить идентификатор сервера, содержащийся в его сертификате ключа проверки электронной подписи. Дальнейшее выполнение протокола выработки ключей зависит от действий сервера. В случае проведения взаимной аутентификации установление соединения не может быть завершено, так как злоумышленник не сможет подделать электронную подпись, содержащуюся в сообщении VerifyMessageи выдать себя за клиента. В случае односторонней аутентификации соединение будет успешно установлено.

***Конфиденциальность.*** Конфиденциальность обеспечивается за счет использования алгоритмов шифрования как на этапе установления соединения, так и в ходе выполнения протокола передачи прикладных данных. Выполнение свойства конфиденциальности передаваемых сообщений следует из выполнения совокупности свойств безопасности: защищенной возможности договориться о параметрах безопасности, подтверждения ключа и аутентификации ключа.

## Заключение

Проведенное исследование позволяет сделать вывод о том, что компрометация криптографических механизмов, регламентируемых Р 1323565.1.028-2019, сводится к компрометации стандартизированных отечественных криптографических решений, а сами криптографические механизмы удовлетворяют всем предъявленным свойствам безопасности.

СПИСОКЛИТЕРАТУРЫ:

1. Ноздрунов В., Семенов А. Подходы к криптографической защите коммуникаций в IoT и M2M. Информационная безопасность, № 5, 2019. С. 38–40. URL: https://infotecs.ru/about/press-centr/publikatsii/podkhody-k-kriptograficheskoy-zashchite-kommunikatsiy-v-iot-i-m2m.html (дата обращения: 23.07.2020).
2. Гребнев С.В., Лазарева Е.В., Лебедев П.А., Нестеренко А.Ю., Семенов А.М. Интеграция отечественных протоколов выработки общего ключа в протокол TLS 1. 3. ПДМ. Приложение, 2018, №11. С. 62–65. DOI:http://dx.doi.org/10.17223/2226308X/11/19.
3. Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E. et al. On post-handshake authentication and external PSKs in TLS 1.3. JComputVirol Hack Tech (2020). DOI: http://dx.doi.org/10.1007/s11416-020-00352-0.
4. Krawczyk H. (2003) SIGMA: The «SIGn-and-MAc»Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols. In: Boneh D. (eds) Advances in Cryptology – CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-540-45146-4_24.
5. Krawczyk H., Paterson K.G., Wee H. (2013) On the Security of the TLS Protocol: A Systematic Analysis. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in

Computer Science, vol. 8042. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-642-40041-4_24.
6. Canetti R., Krawczyk H. (2001) Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In: Pfitzmann B. (eds) Advances in Cryptology – EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/3-540-44987-6_28.
7. Semenov A.M.,Analysis of Russian key-agreement protocols using automated verification tools, Матем. вопр. криптогр.,2017.Т. 8, вып. 2. P. 131–142. DOI: http://dx.doi.org/10.4213/mvk229.
8. E.K. Alekseev, V.D. Nikolaev, S.V. Smyshlyaev, On the security properties of Russian standardized elliptic curves, Матем. вопр. криптогр., 2018. Т. 9, вып. 3. P. 5–32.DOI: http://dx.doi.org/10.4213/mvk260.
9. A.Yu. Nesterenko, Construction of strong elliptic curves suitable for cryptographic applications, Матем. вопр. криптогр., 2019. Т. 10, вып. 2. P. 135–144. DOI:http://dx.doi.org/10.4213/mvk291.
10. D. Dolev and A. Yao, "On the security of public key protocols," in IEEE Transactions on Information Theory, vol. 29, no. 2. P. 198–208, March 1983. DOI: http://dx.doi.org/10.1109/TIT.1983.1056650.
11. Черемушкин А.В., «Криптографические протоколы: основные свойства и уязвимости», ПДМ, 2009, приложение № 2. С. 115–150.
12. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997.
13. А.Ю. Нестеренко, Об одном подходе к построению защищенных соединений, Матем. вопр. криптогр., 2013. Т. 4, вып. 2. С. 101–111.DOI: http://dx.doi.org/10.4213/mvk86.
14. Горбатов Виктор С., Жуков Игорь Ю., Мурашов Олег Н. Криптографический протокол аутентификации и выработки общего ключа контрольных устройств автотранспорта. Безопасность информационных технологий, [S.1.]. Т. 24. № 4. С. 27–34, 2017. DOI: http://dx.doi.org/10.26583/bit.2017.4.03.
15. Нестеренко А.Ю. Новый протокол выработки общего ключа. Системы высокой доступности. № 2. 2012. С. 81–90.
16. Tristan Ninet. Formal verification of the Internet Key Exchange (IKEv2) security protocol. Cryptography and Security [cs.CR]. Université Rennes 1, 2020. HAL Id: tel-02882167.
17. Avalle, M., Pironti, A. &Sisto, R. Formal verification of security protocol implementations: a survey. Form Asp Comp 26, P. 99–123 (2014). DOI: http://dx.doi.org/10.1007/s00165-012-0269-9.
18. W. Diffie, M. Hellman,“New directions in cryptography,” in IEEE Transactions on Information Theory? vol. 22, no. 6. P. 644–654. November 1976. DOI: http://dx.doi.org/10.1109/TIT.1976.1055638.
19. Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В. О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, Матем. вопр. криптогр., 2016. Т. 7, вып.1. С. 5–38. DOI: http://dx.doi.org/10.4213/mvk172.

REFERENCES:

[1] Nozdrunov V., Semenov A. Approaches to cryptographic protection of communications in IoT and M2M. Information security, № 5, 2019. P. 38–40. URL: https://infotecs.ru/about/press-centr/publikatsii/podkhody-k-kriptograficheskoy-zashchite-kommunikatsiy-v-iot-i-m2m.html (accessed: 23.07.2020) (in Russian).
[2] Grebnev S.V., Lazareva E.V., Lebedev P.A., NesterenkoA.Yu., Semenov A.M. Integration of russian key-agreement protocols into the TLS 1. 3. PDM. Application, 2018, №11. P. 62–65. DOI: http://dx.doi.org/10.17223/2226308X/11/19.
[3] Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E. et al. On post-handshake authentication and external PSKs in TLS 1.3. J ComputVirol Hack Tech (2020). DOI: http://dx.doi.org/10.1007/s11416-020-00352-0.
[4] Krawczyk H. (2003) SIGMA: The «SIGn-and-MAc» Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols. In: Boneh D. (eds) Advances in Cryptology – CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-540-45146-4_24.
[5] Krawczyk H., Paterson K.G., Wee H. (2013) On the Security of the TLS Protocol: A Systematic Analysis. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, vol. 8042. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/978-3-642-40041-4_24.
[6] Canetti R., Krawczyk H. (2001) Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In: Pfitzmann B. (eds) Advances in Cryptology – EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045. Springer, Berlin, Heidelberg. DOI: http://dx.doi.org/10.1007/3-540-44987-6_28.

[7] Semenov A.M., Analysis of Russian key-agreement protocols using automated verification tools, Mat. Vopr. Kriptogr., 2017. Vol. 8, Issue 2. P.131–142. DOI: http://dx.doi.org/10.4213/mvk229.
[8] E.K. Alekseev, V.D. Nikolaev, S.V. Smyshlyaev, On the security properties of Russian standardized elliptic curves, Mat. Vopr. Kriptogr., 2018. Vol. 9, Issue 3. P. 5–32. DOI: http://dx.doi.org/10.4213/mvk260.
[9] A.Yu. Nesterenko, Construction of strong elliptic curves suitable for cryptographic applications, Mat. Vopr. Kriptogr., 2019. Vol. 10, Issue 2. P. 135-144. DOI: http://dx.doi.org/10.4213/mvk291.
[10] D. Dolev and A. Yao, "On the security of public key protocols," in IEEE Transactions on Information Theory, vol. 29, no. 2. P. 198–208, March 1983. DOI: http://dx.doi.org/10.1109/TIT.1983.1056650.
[11] Cheremushkin A.V., Cryptographic protocols: basic properties and vulnerabilities, PDM, 2009, application № 2, P. 115–150 (in Russian).
[12] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997.
[13] A.Yu. Nesterenko, On an approach to the construction of secure connections, Mat. Vopr. Kriptogr., 2013. Vol. 4, Issue 2. P. 101–111. DOI: http://dx.doi.org/10.4213/mvk86 (in Russian).
[14] GorbatovViktorS., ZhukovIgorY., MurashovOlegN. Authentication and common key generation cryptographic protocol for vehicle tachographs. IT Security, [S.1.]. Vol. 24, no. 4. P. 27–34, 2017. DOI: http://dx.doi.org/10.26583/bit.2017.4.03 (in Russian).
[15] Nesterenko A.YU. The new Protocol develop common key. Sistemy vysokoj dostupnosti. № 2. 2012. P. 81–90 (in Russian).
[16] Tristan Ninet. Formal verification of the Internet Key Exchange (IKEv2) security protocol. Cryptography and Security [cs.CR]. Université Rennes 1, 2020. HAL Id: tel-02882167.
[17] Avalle, M., Pironti, A. &Sisto, R. Formal verification of security protocol implementations: a survey. Form Asp Comp 26. P. 99–123 (2014). DOI: http://dx.doi.org/10.1007/s00165-012-0269-9.
[18] W. Diffie, M. Hellman, “New directions in cryptography,” in IEEE Transactions on Information Theory? Vol. 22, no. 6. P. 644–654. November 1976. DOI: http://dx.doi.org/10.1109/TIT.1976.1055638.
[19] E.K. Alekseev, I.B. Oshkin, V.O. Popov, S.V. Smyshlyaev, On the cryptographic properties of algorithms accompanying the application of standards GOST R 34.11-2012 and GOST R 34.10-2012, Mat. Vopr. Kriptogr., 2016. Vol.7, Issue1. P. 5–38. DOI: http://dx.doi.org/10.4213/mvk172 (in Russian).

*Поступила в редакцию - 13 июля 2020 г. Окончательный вариант – 01 ноября 2020 г.*
*Received –July13, 2020. The final version – November 01, 2020.*