**УДК 003.26**

*А. М. Желудкова**

# ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА

Благодаря научно-техническому прогрессу человечество совершает множество открытий. Но неизбежным следствием этого является то, что состояние экологии в развитых и развивающихся странах сильно ухудшается, что, в свою очередь, оказывает значительное влияние на людей. Уже в прошлом веке государства и международные организации пытались взять контроль над данной ситуацией. Примером подобной деятельности можно считать Киотский договор, призванный уменьшить выброс парниковых газов в атмосферу.

Для наблюдения используется система экологического мониторинга (ЭМ). При этом соблюдение всех условий Киотского договора несет за собой большие траты на оборудование и крупные штрафы за их нарушение этих условий. В связи с этим, существует большое количество заинтересованных в фальсификации результатов экологического мониторинга [1].

Эта проблема могла бы быть решена путем шифрования данных, передаваемых станциями ЭМ. Но станции находятся на территории отдельных стран, а данные передаются за границу в международные организации. Правительства этих стран вправе требовать передачи ключей шифрования, чтобы исключить возможность передавать разведывательную информацию под видом данных экологического мониторинга. Но в таком случае возникает риск изменения передаваемых данных любым из владельцев ключа шифрования.

Задача обеспечения станций ЭМ средствами защиты информации о состоянии окружающей среды от изменения при одновременной доступности содержания этой информации для всех заинтересованных лиц является весьма актуальной. Эта задача может быть решена методами асимметричного шифрования, известными с 1977 г. [2].

Данные на станции ЭМ будут зашифрованы секретным ключом, а получатель сможет расшифровать их, используя открытый ключ. Благодаря этому будет невозможна модификация данных, передавае-

* Работа выполнена под руководством канд. техн. наук, доц. ФГБОУ ВО «ТГТУ» В. А. Гриднева.

мых со станций ЭМ, а их содержание останется доступным для всех заинтересованных субъектов.

Для реализации такого шифрования целесообразно использовать метод эллиптических кривых (ЭК). Выбор обусловлен тем, что по сравнению с другими алгоритмами асимметричного шифрования (RSA, Эль-Гамаля), требуемая надежность ключа будет обеспечиваться его меньшим размером [3], что обеспечивает высокую скорость криптографических преобразований и сравнительно невысокие требования к аппаратным средствам. Все это позволит использовать алгоритм асимметричного шифрования в условиях технических ограничений станций ЭМ.

Общая идея криптографической защиты данных экологического мониторинга выглядит следующим образом. Допустим, на станции уже заданы параметры уравнения кривой, принятые для системы ЭМ. На станции ЭМ генерируется пара ключей – секретный и открытый. Для удобства, открытый ключ можно передавать вместе с сообщением. Это обеспечивает возможность ознакомления с передаваемой информацией всех заинтересованных субъектов. Закрытый ключ известен только станции ЭМ, что позволяет обеспечить защиту передаваемых данных от модификации.

Станция ЭМ формирует пакет сообщения, включающий измеренные показатели состояния окружающей среды, свой идентификатор ID, метку времени T и шифрует его своим секретным ключом. Затем к зашифрованному сообщению добавляется открытый ключ и контрольная сумма. Контрольная сумма позволяет проверять целостность принятого сообщения без необходимости его расшифрования. Структура передаваемого пакета показана на рис. 1.


**Рис. 1. Структура передаваемого пакета**

На приемной стороне полученное сообщение проверяется на отсутствие случайных искажений при передаче по каналу связи путем верификации контрольной суммы. В случае отрицательного результата верификации, сообщение отклоняется с возможностью запроса повторной передачи. При успешной верификации контрольной суммы сообщение расшифровывается с помощью открытого ключа. Затем проводится верификация метки времени для исключения атаки типа повтора ранее переданного сообщения. При несовпадении метки вре-

мени сообщение отклоняется, а при успешной верификации принятые данные используются по предназначению [4].

Описанная выше идея реализована в разработанном прикладном программном обеспечении (ПО), включающем три автономных модуля: генерации ключей, передающий и приемный.

Организация, отвечающая за обслуживание станции ЭМ, задает на ней параметры ЭК, таких как: модуль; простое число, обозначающее порядок циклической подгруппы группы точек ЭК; коэффициенты уравнения ЭК; координаты базовой точки. На основании этих параметров модуль генерации ключей будет автоматически генерировать пару ключей – секретный (для зашифрования) и открытый (для расшифрования).

Передающий модуль программы на станции ЭМ проводит необходимые криптографические преобразования измеренных данных экологического мониторинга, формирует пакет сообщения, вид которого показан на рис. 1 и отправляет его в международную организацию.

Приемный модуль разработанного ПО содержит те же параметры криптосистемы, что и передающий модуль. В интерфейсе приемного модуля разработанного ПО предусмотрены поля для указания пути к файлу, подлежащему расшифрованию и содержащему открытый ключ для расшифрования.

Приемный модуль разработанного ПО после предварительной обработки принятого пакета сообщения проводит его проверку на предмет случайных искажений путем верификации контрольной суммы. В случае обнаружения ошибок, выполняется автоматический перезапрос передачи пакета. При успешной верификации контрольной суммы принятый пакет передается для дальнейшей обработки.

После расшифрования принятого сообщения приемный модуль ПО проводит верификацию метки времени. Если для расшифрованного сообщения фиксируется несоответствие метки времени, то данное сообщение стирается. Если же верификация метки времени прошла успешно, то принятое сообщение передается для использования по предназначению.

Текст принятого сообщения выводится в специальном окне программы, но при необходимости его можно сохранить в виде отдельного файла. Для этого в приемном модуле разработанного ПО предусмотрено указание пути сохранения файла.

Невозможность корректного расшифрования принятого сообщения при соблюдении всех вышеуказанных условий будет однозначно свидетельствовать о его несанкционированной умышленной модификации. В этом случае принятое сообщение уничтожается, и формируется запрос на его повторную передачу.

Так же предусмотрена возможность записи происходящих событий в специальный, защищенный от модификаций журнал. В нем будет храниться информация об ID станций ЭМ, принятых от этих станций сообщениях и обнаруженных в них ошибках.

Окно интерфейса приемного модуля разработанного ПО показано на рис. 2.

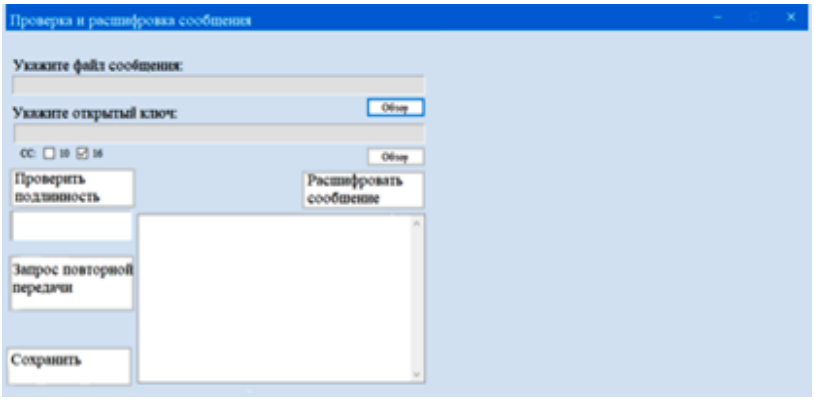


**Рис. 2. Интерфейс приемного модуля программного обеспечения**

Приведенный вид окна интерфейса не является окончательным, возможна его доработка. В правом поле планируется сделать поля для вывода сообщений об ошибках и перезапросах.

## Список литературы

1. Латышенко, К. П. Экологический мониторинг / К. П. Латышенко. – М. : Юрайт, 2016. – 376 с.

2. Жданов, О. Н. Эллиптические кривые. Основы теории и криптографические приложения / О. Н. Жданов, В. А. Чалкин. – М. : Либроком, 2012. – 200 с.

3. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С / Б. Шнайер. – М. : Вильямс, 2016. – 1024 с.

4. Feghhi, J. Digital Certificates: Applied Internet Security / J. Feghhi, P. Williams. – Boston : Addison-Wesley Professional, 1998. – 480 p.

*Кафедра «Информационные системы и защита информации»*
*ФГБОУ ВО «ТГТУ»*