УДК 003.26

*А. М. Желудкова**

О КРИПТОЗАЩИТЕ ДАННЫХ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА

В наши дни человечество совершает одно открытие за другим. Экологическая обстановка в развитых и развивающихся странах становится все хуже, что существенно влияет на здоровье человека. Еще с прошлого столетия государства стали предпринимать попытки контроля данной ситуации. Одной из таких попыток стал Киотский договор, призванный снизить сокращение выбросов парниковых газов в атмосферу. Для контроля выбросов используется система экологического мониторинга (ЭМ). Проблема в том, что соблюдение условий договора влечет за собой дополнительные траты на очистные сооружения и штрафы за нарушения. Следовательно, большое количество людей заинтересовано в подделке результатов экологического мониторинга [1].

Задача состоит в обеспечении станций ЭМ средствами защиты информации о состоянии окружающей среды от изменения или, как говорят, обеспечения их аутентичности. Это можно было бы сделать с помощью шифрования. Но станции экологического мониторинга расположены на территории суверенных государств, а данные от них передаются в международные организации. Поэтому спецслужбы могут потребовать предоставления им ключа шифрования для исключения возможности передачи разведывательной информации. Но сторона, располагающая ключом шифрования, может влиять на содержание передаваемых данных, нарушая их аутентичность.

Проблема может быть решена при использовании асимметричного шифрования. Данные на станции ЭМ будут зашифрованы секретным ключом, а получатель сможет расшифровать их, используя открытый ключ. Благодаря этому любой заинтересованный субъект сможет ознакомиться с содержанием данных экологического мониторинга, а модификация этих данных будет невозможна.

Для шифрования предлагается использовать алгоритм на основе эллиптических кривых (ЭК). Выбор алгоритма обусловлен тем, что по

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

сравнению с другими алгоритмами асимметричного шифрования (RSA, Эль-Гамаля), определенная надежность ключа будет обеспечиваться его меньшим размером [2]. Скорость криптографических преобразований также будет значительно выше, что позволит использовать их в условиях технических ограничений станций ЭМ.

Допустим, для нужд ЭМ заданы параметры уравнения кривой. Станция генерирует пару закрытый–открытый ключ. Сообщение, зашифрованное секретным ключом, можно расшифровать открытым ключом. Вычисление секретного ключа по открытому ключу относится к труднорешаемым задачам. Открытый ключ рассылается на принимающую сторону для расшифровки сообщения или помещается в публичный справочник. Для удобства открытый ключ можно отправлять вместе с сообщением. Закрытый ключ известен только станции ЭМ, что позволяет обеспечить аутентичность передаваемых данных.

Текст или отдельный блок сообщения, как обычно при асимметричном шифровании, переводится в числовую форму и приводится к целочисленному виду. На ЭК получаем координаты точки, которые шифруются и передаются.

Благодаря открытому ключу на приемной стороне можно будет восстановить сообщение.

Помимо этого, предлагается использовать в сообщении несколько меток: метка времени, идентификатор станции ЭМ, случайное число. Метка времени необходима для предотвращения повторения сообщений. Каждое новое сообщение будет иметь другую метку времени. Каждая станция имеет уникальный идентификатор, а случайное число заранее известно и является параметром системы наряду с коэффициентами уравнения эллиптической кривой.

Станция ЭМ шифрует измеренные показатели, добавляет к ним метку времени, идентификатор и случайное число. Станция вычисляет значение хэш-функции из идентификатора и случайного числа. Это значение вместе с меткой времени и идентификатором отправляются в организацию. Организация по метке времени проверяет сообщение на наличие атаки типа повтора. Далее по базе находят соответствие идентификатора и случайного числа. На их основе вычисляется значение хэш-функции и сравнивается со значением, принятым от станции [4].

Таким образом, можно сделать вывод о том, что использование меток времени, случайного числа и идентификатора станции исключает возможность повтора ранее переданных сообщений, а асимметричное шифрование позволяет исключить подмену данных. Подобная схема может найти применение в любой системе, требующей исключения постороннего вмешательства.

Ранее уже говорилось о технической ограниченности станций ЭМ. Предполагается создание небольшого аппаратного модуля, который решил бы эту проблему, и программного обеспечения для него.

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 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.

Продажа оборудования и лицензии на ПО позволит коммерциализовать проект. Так же возможна продажа прав компаниям производителям оборудования ЭК для последующей реализации.

В таблице 1 представлена смета проекта.

1. Смета проекта

Наименование предполагаемых расходов	Сумма, руб.
Патентные исследования	40 000
Обоснование требований к проектируемой системе	40 000
Разработка прикладного ПО генерации ключей, асимметричного шифрования и расшифрования	100 000
Тестирование разработанного ПО, включая моделирование атак	90 000
Приобретение деталей для сборки аппаратного модуля	8000
Сборка и тестирование аппаратного модуля	52 000
Подготовка научной статьи по результатам работы	50 000
Публикация в научном журнале «Вопросы современной науки и практики»	6000 (979 р. 40 коп. за страницу)
Подготовка пакета документов для регистрации разработанного ПО и оборудования	4000
Затраты на регистрацию разработанного прикладного ПО и оборудования, включая госпошлину	10 000
Итого	**400 000**

Список литературы

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

2. Tanenbaum, A. Computer Networks / A. Tanenbaum, D. Wetherall. – London : Pearson, 2010. – 960 p.

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

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

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

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