

**СЕКЦИЯ 3**  
**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И МОДЕЛИРОВАНИЕ**  
**ЭКОНОМИЧЕСКИХ ПРОЦЕССОВ ПРИ ОБОСНОВАНИИ**  
**ЭФФЕКТИВНЫХ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ**

УДК 004.056

**Н. Амбросов**

(Республика Беларусь)

Научный руководитель: Л.И. Крошинская, доцент  
БИП-Институт правоведения

**ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ**

В Законе Республики Беларусь № 353-З от 10 января 2000 года «Об электронном документе» дается следующее определение электронного документа: «Электронный документ — это документ, подготовленный с использованием системы электронного документооборота, зафиксированный на материальном носителе в виде объекта системы электронного документооборота (СЭД) и снабженный реквизитами, с помощью которых можно идентифицировать место, время создания и автора документа».

Одним из реквизитов электронного документа является электронная цифровая подпись (ЭЦП), которая является аналогом собственноручной подписи в электронном виде и является полноценной заменой собственноручной подписи в случаях, предусмотренных законом. Если документ содержит ЭЦП, то он юридически считается оригиналом.

Наличие ЭЦП доказывает, что документ подписан автором, так как создать корректную подпись можно, лишь зная закрытый ключ, который известен только владельцу. ЭЦП дает возможность контролировать целостность пересылаемого документа и защитить его от изменений, так как при любом изменении документа подпись станет недействительной.

Каждому участнику электронного обмена документами, генерируются уникальные открытый и закрытый (секретный) криптографические ключи.

Значение ЭЦП получается в результате криптографического преобразования информации с использованием закрытого ключа. Закрытый ключ хранится у автора документа и с его помощью производится шифрование и формируется ЭЦП.

Путем криптографического преобразования с использованием содержимого документа и закрытого ключа создается некоторая произвольная последовательность символов. Эта последовательность символов и является ЭЦП пользователя под данным конкретным документом. ЭЦП может храниться как в отдельном файле, так и добавляться в конец отправляемого

го электронного документа. В ЭЦП содержатся: имя файла открытого ключа; данные о лице, сформировавшем подпись; дата ее формирования.

Для проверки подлинности ЭЦП используется открытый ключ. Получатель документа имеет открытый ключ отправителя, с помощью которого выполняется обратное криптографическое преобразование, а также проверка ЭЦП отправителя. Если при проверке ЭЦП под документом верна, то это значит, что в текст не был изменен и документ подписан автором, если это не так, то будет выдано сообщение, что сертификат отправителя не действителен.

Для управления открытыми ключами необходимо:

- обеспечить доступ пользователей к подлинному открытому ключу любого другого пользователя;
- защитить эти ключи от подмены;
- организовать отзыв ключа в случае его компрометации.

Задача защиты открытых ключей решается с помощью сертификатов, подписанных доверенным лицом и позволяющих удостовериться в том, что данные о владельце и его открытом ключе. Для этого используются центры сертификации, где пользователь может получить сертификат какого-либо пользователя, а также проверить, не отозван ли необходимый открытый ключ.

Если закрытый ключ будет украден или потерян, то кто-либо может создать действительную цифровую подпись любого электронного документа от лица владельца ЭЦП. При краже или потере ЭЦП она может быть немедленно отозвана. Ответственность за сохранность закрытого ключа несет сам владелец.

В соответствии с законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» от 28 декабря 2009 года №113-З сертификаты открытых ключей, изданные в Государственной системе управления открытыми ключами проверки электронной цифровой подписи, обязательны к применению при обращении электронных документов во всех государственных информационных системах, а также в иных информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено.

В Беларуси в июне 2014 года был создан Республиканский удостоверяющий центр (РУЦ) Государственной системы управления открытыми ключами проверки электронной цифровой подписи, который входит в структуру Республиканского унитарного предприятия (РУП) «Национальный центр электронных услуг». Для проверки подлинности ЭЦП используется открытый ключ. Удостоверяющий центр обеспечивает регистрацию и надежное хранение открытых ключей во избежание внесения искажений или попыток подделки. В удостоверяющем центре находится

дубликат открытого ключа, создана библиотека сертификатов открытых ключей.

Использование электронной цифровой подписи позволит создать условия для дальнейшего развития электронного документооборота, в том числе электронного декларирования, повысить эффективность механизмов реализации принципа «одно окно».

УДК 339.18:519.8

**Д. Башко**

(Республика Беларусь)

Научный руководитель: Е.И. Подашевская, ст. преподаватель  
Белорусский государственный аграрный технический университет

### **ЭКОНОМИКО-МАТЕМАТИЧЕСКИЕ МЕТОДЫ ДЛЯ РЕШЕНИЯ ЗАДАЧИ РАСПРЕДЕЛИТЕЛЬНОЙ ЛОГИСТИКИ**

В распределительной логистике наряду с задачами распределения материальных потоков выделяются задачи распределения трудовых ресурсов. Это актуально, поскольку даёт возможность экономии как временных, так и денежных ресурсов. Рассмотрим применение методологии экономико-математического моделирования для решения по распределению рабочих.

Требуется собрать бригаду рабочих для работы, состоящей из нескольких операций. Каждый рабочий может выполнять любую операцию, но затраты времени на ее выполнение различаются. Цель задачи – обеспечить выполнение заданного объема работ с минимальными затратами времени.

В рассматриваемом примере требуется 2 раза выполнить 5 операций. Количество операций, выполняемых одним работником, можно ограничить – не более 3 операций. Общее время выполнения работ – 96 часов.

Алгоритм выполнения задачи следующий.

1. В Excel заносятся исходные данные о времени выполнения рабочими (P1...P14) требуемой операции (O1...O5). В примере используются ячейки C3...G16.

2. Создаётся рабочая матрица (рис. 1), в которой будет отображаться распределение рабочих по выполняемым операциям и суммарное время выполнения операций каждым работником, а также общее время выполнения операции (96 часов). Целевая функция (H32) – это сумма произведений рабочей матрицы B18...F31 на матрицу исходных данных C3...G16.