Азарова А. А., Ивчук К. В., Кукуруза М. И

Азарова Анжелика Алексеевна (azarova.angelika@mail.ru),к.т.н., заместитель директора Института менеджмента Винницкого национального технического университета, профессор кафедры менеджмента и безопасности информационных систем; Ивчук Екатерина Витальевна, студентка Винницкого национального технического университета; Кукуруза Марина Игоревна, студентка Винницкого национального технического университета.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИОННОЙ МОДЕЛИ ПРЕДПРЯТИЯ

В статье рассмотрены основные аспекты построения и использования информационной модели, которая функционирует в организациях. Обоснована целесообразность использования для защиты внутриорганизационной информации электронную цифровую подпись.

Ключевые слова: организация, информационная модель, электронная цифровая подпись.

Введение. Функционирования производственных и экономических объектов определяется их способностью удовлетворять те или иные потребности общества. Каждый такой объект вступает в определенные отношения с изменяющейся внешней средой (с государственными органами управления и др.) и состоит из множества различных элементов, взаимодействие которых и обеспечивает его существование и выполнение своих функций.

В дальнейшем будем называть любой такой объект независимо от его размеров, формы собственности, организационно-правового статуса организацией.

Организация - это стабильная формальная социальная структура, которая получает ресурсы из окружающего мира и перерабатывает их в продукты своей деятельности. Всем организациям присущи как индивидуальные так и общие черты.

Результатом взаимодействия организации со средой являются изменения различного рода, которые вызывают необходимость управления - такого целенаправленного воздействия на организацию, которое обеспечит достижение поставленных целей. Управление позволяет в зависимости от особенностей конкретных организаций и целей стабилизировать их, сохранить качественную определенность, поддержать динамическое равновесие со средой, обеспечить совершенствование организации и достижение того или иного полезного эффекта.

Организация имеет внутренние информационные связи (взаимодействие руководства с подчиненными и исполнителями) и внешние информационные связи (взаимодействие с контролирующими органами, смежными предприятиями, потребителями и др.).

Система информационного обеспечения осуществляет информационную поддержку деятельности организации по всем направлениям служебной деятельности, предоставляя многоцелевую статистическую, аналитическую и справочную информацию.

Изложение основного материала. Организация работы с данными - это один из главных этапов создания прикладних програм. Именно от этого первого этапа, который часто недооценивается, зависит создание всей системы автоматизированной обработки данных и успех ее эксплуатации у конечного потребителя.

Для обсуждения этой проблемы необходимо рассмотреть определенные аспекти теории информационных систем, а именно средства описания организации данных - информационные модели, и средства их защиты - электронно-цифровую подпись.

Информационные модели (ИМ) - это средство формирования представления о данных, их состав и использование в конкретных условиях.

В деятельности любой организации важное место занимает работа с документами, которые необходимо получать извне, готовить внутри организации, регистрировать, передавать работникам, контролировать выполнение, вести справочную работу, сохранять. Организация работы с документами является важной составной частью процессов управления и принятия управленческих решений, которая существенно влияет на оперативность, экономичность и надежность функционирования аппарата управления учреждения, культуру труда управленческого персонала и качество управления.

Информационная модель организации является схемой потоков информации, используемой в процессе управления, отражает различные процедуры выполнения функций управления организацией и представляет по каждому заданию связь входящих и исходящих документов и показателей.

Информационная модель организации ориентирована на информацию как ресурс, который производится и используется в процессе функционирования системы управления, направленная на решение информационных проблем, рационализацию и интеграцию информационных процессов, улучшение организационной структуры, повышение эффективности работы в целом [1] .

На сегодня решение проблемы защиты информации различного рода на предприятиях осуществляется путем использования электронной цифровой подписи (ЭЦП), которая позволяет осуществлять аутентификацию как автора электронного документа, так и самого документа. По мнению авторов, это дает возможность использовать ЭЦП как аналог собственноручной подписи для придания электронному документу юридической силы. Поэтому ЭЦП является средством защиты информационной модели организации.

Для функционирования ЭЦП используются два ключа защиты (хранящиеся в разных файлах) :

- тайный ключ, который хранится у адресанта;

- открытый ключ, который, как правило, публикуется в общедоступном или специализированном справочнике [2] .

Для наложения ЭЦП используется секретный (личный) ключ, а для его проверки - открытый (общеизвестный) ключ.

Алгоритм работы системы построен таким образом, что имея доступ к открытому ключу невозможно восстановить секретный ключ или поставить цифровую подпись - ее можно только проверить.

Следует заметить, что секретный ключ адресанта является полной личной его собственностью и не передается любым другим персонам (даже центру сертификации ключей). Любой может проверить цифровую подпись, используя только открытый ключ. Наложение электронной цифровой подписи - это операция, которая осуществляется отправителем документа с использованием его секретного ключа. При выполнении этой операции на вход соответствующей программы подаются данные, которые необходимо подписать, и секретный ключ подписывающего. Программа создает из данных с помощью секретного ключа уникальный блок данных фиксированного размера, который может быть действительным только для этого тайного ключа и именно для этих входных данных. То есть ЭЦП - это своеобразное цифровое отражение секретного ключа и документа [3].

В дальнейшем ЭЦП, как правило, добавляется к исходному документу (или размещается в отдельном поле документа), и такая комбинация данных (документ + ЭЦП) создает защищенный электронный документ.

Среди наиболее распространенных и актуальных прикладных задач, которые решаются в организациях с помощью цифровой подписи, являются:

- обеспечение безопасности электронного документооборота;

- обеспечение безопасности электронных платежных систем и электронной коммерции;

- обеспечение авторства при электронном голосовании;

- подписывание сообщений электронной почты;

- аутентификация в беспроводных сетях;

- обеспечение безопасности мобильной коммерции;

- обеспечение безопасности сотовой связи;

- подписи цифровых сертификатов и цифровых паспортов на базе смарт-карт.

С точки зрения авторов при применении методов цифровой подписи для решения рассмотренных выше задач возникает проблема, связанная с тем, что практически во всех этих задачах проверку цифровой подписи необходимо осуществлять значительно чаще, чем ее формирование. В этом случае проверяющая сторона может получать большое количество запросов на проверку подписи, в свою очередь может приводить к перезагрузке системы, выполняющей такую проверку [4] .

Выводы. Электронная цифровая подпись является тем инструментом, который дает возможность создать правовые основы для электронного документооборота, заключать сделки, создавать платежные системы нового типа, электронные ценные бумаги и т. п. Она используется для подтверждения целостности, действительности и авторства любых электронных документов: текстовых, графических, отдельных строк или записей в базах данных и т.д.

Такая подпись по правовому статусу приравнивается к собственноручной подписи (печати) в случае, если:

- электронная цифровая подпись подтверждена с использованием усиленного сертификата ключа с помощью надежных средств цифровой подписи;

- при проверке использовался усиленный сертификат ключа, действующий на момент наложения электронной цифровой подписи;

- личный ключ подписанта соответствует открытому ключу, указанном в сертификате.

Цифровая подпись становится все более и более популярной, в основном, благодаря быстрому развитию цифрового обмена данными. Использование электронной цифровой подписи и ее надлежащая проверка при принятии документа минимизируют возможность подделок электронного документа, то есть приравниваются к собственноручной подписи и печати организации.

Таким образом автори доказывают целесообразность использования ЭЦП для обеспечения деятельности физических и юридических лиц, осуществляемой с использованием электронных документов .

Литература:

1. Матвієнко О., Цивін М. Основи організації електронного документообігу: навч. посібник / А. Матвієнко, М. Цивін . - К. : Центр навчальної літератури, 2008 . – 112 с .

2. Лужецький В. А. Інформаційна безпека: посібник / В. А. Лужецький, А. П. Войтович, А.В. Дудатьєв . - М. : Університ -Вінниця , 2009. - 240 с.

3. Гніліцький В. В. Захист інформації : навч. посібник для студентів економічних спеціальностей / В. В. Гніліцький, Є. Г. Орєхов. - М. : ІМІДЖ, 2009. - 164 с.

4. Єрохін К. Актуально про електронну звітність / К. Єрохін. - К.: Державний комітет телебачення і радіомовлення України , 2007. - 212 с.