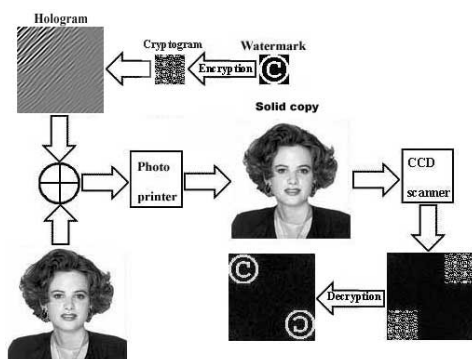


Важнейшим элементом любой информационной системы является шифрование конфиденциальной информации. Рассматриваемый подход не является исключением - двумерные криптограммы органически встраиваются в цепочку преобразований двумерных изображений (смотри рисунок):



Стойкость шифра определяется исключительно стойкостью секретного ключа. Таким образом, аналоговое исполнение средства защиты объекта идентификации (фотографии владельца) и скрытый характер встраиваемых данных представляет собой малопривлекательный объект для цифрового взлома, а подключение криптографической под-

системы к стеганографической системе сокрытия данных обеспечивает мощный барьер несанкционированному вмешательству.

В заключение, стоит отметить, что предложенную технологию можно рассматривать как дополнительную степень защиты документов к существующим технологиям. И в этом смысле, на PhotoWaterMark возлагается защита фотографических материалов на аналоговом уровне, а за микрочипами остается их неоспоримое преимущество - простой и удобный способ работы с цифровыми массивами данных.

## "TIME CARD" - БЕЗОПАСНОСТЬ ВАШЕЙ КОМПАНИИ В ВАШИХ РУКАХ!

**Станислав ЖУК, Евгения ЗГАРДАН**  
Теоретический Лицей им. "Михаил Когэлничану"  
(Республика Молдова)

*Information security is the process of protecting information. It protects its availability, privacy and integrity. "TIME CARD" - the software for the account of working hours of the personnel of the company which possesses following advantages: gives possibility of automation of the account of working hours and protection against deliberate infringement of the data.*

Кто владеет информацией, тот владеет миром! Пренебрежение этой истиной может обойтись в миллионы и миллиарды убытков. Даже в современной истории можно найти массу красноречивых примеров, когда один единственный файл или документ вершил судьбы сотен тысяч людей и целых корпораций. В силу этих причин защита информации сегодня многими бизнес структурами считается главным

направлением деятельности в области внедрения технологий корпоративной безопасности. Не смотря на это, многие бизнесмены считают, что защитить от кражи папку с бумагами можно, поставив надежный замок на сейф, а защита данных в электронном виде заключается лишь в установке пароля на компьютер. Тем не менее, любая система управления документами и защиты данных — это не просто ограничение доступа к файлам или бумагам. Это современные технологии, которые обеспечивают непрерывность бизнес процессов путем создания электронного архива, внеофисного хранения информации, а также других методов программного и аппаратного типа.

Безопасность информации сегодня не роскошь и не причуда руководства, а вопрос «обезопасить или не обезопасить?» даже не поднимается - ответ очевиден, как очевидна необходимость чистить зубы утром и вечером. Говорят лишь об уровнях безопасности, а они различны.

Насколько уязвим ваш бизнес и вы сами, когда кто-то посторонний имеет возможность доступа к вашей информации? Что сделают ваши конкуренты, журналисты, недруги и мошенники, получив конфиденциальную информацию о вашем бизнесе?

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

Мы предлагаем вам один из возможных способов решения этой проблемы. "Time Card"-программное обеспечение для учета рабочего времени персонала компании, которое обладает следующими преимуществами:

- Предоставляет возможность автоматизации учета рабочего времени;
- Полноценное ведение табельного учета в электронных табельных журналах, пользуясь всеми возможностями автоматического заполнения;
- Ограничение доступа пользователей к табелю согласно штатному расписанию компании.
- Защита от преднамеренного нарушения данных;
- Хранение табелей непосредственно в базе данных;
- Возможность получения оперативных отчетов по учету трудозатрат.

Защита от преднамеренного нарушения данных представленного нами продукта состоит в следующем:

После того как вы установили программу, вы получаете доступ к единой базе данных, единому архиву. И так, Вы директор компании X. С помощью данного продукта, вы получаете возможность заполнения, редактирования и просмотра своего табеля рабочего времени, а также табелей подчиненных.

Для обеспечения эффективной защиты информации предусмотрен контроль на трех основных уровнях:

- контроль доступа к информации со стороны пользователей информационной системы;
- контроль физической сохранности баз данных и их непротиворечивости;
- контроль конфиденциальности передаваемых по сетям данных и работоспособности сетевой инфраструктуры.

#### **Средства обеспечения безопасности.**

1. Обычная практика предполагает аутентификацию (распознавание) пользователей с помощью паролей.
2. Проверка полномочий при доступе к бизнес-объектам.

Например, для конкретного бухгалтера на предприятии в соответствии с его ролью может быть открыта возможность доступа к выполнению проводки бухгалтерского документа, но только на уровне своей бизнес-единицы, по конкретной группе счетов или по операциям отдельных деловых партнеров. Если у пользователя нет необходимых полномочий, система отказывает в получении доступа к соответствующим транзакциям или документам.

3. Администрирование ролей пользователей.

Для того, чтобы упростить ведение детальных данных полномочий каждого пользователя, предусмотрен специальный инструмент – генератор профилей полномочий. Основная идея заключается в использовании стандартных ролей бизнес-пользователей в соответствии с их должностными ролями. Вы можете, например, присвоить отдельному сотруднику одну или несколько стандартных ролей, и этим полностью определить профиль его полномочий. При необходимости Вы можете отредактировать перечень функций, добавив или удалив один объект полномочий или целую группу функций.

Ограничения полномочий пользователя не являются гарантией корректности данных бизнес-документов. В случае, если все действия пользователя документируются и существует формальное подтверждение автора изменений, Вы можете контролировать источник данных и, как следствие, управлять ответственностью за конкретные действия пользователей.

4. Защита одновременного доступа к изменению данных.

“TIME CARD” также обеспечивают защиту одновременного доступа к объектам многопользовательской обработки с помощью механизмов блокировки.

Эти механизмы предотвращают одновременный доступ нескольких пользователей к одному и тому же объекту через транзакцию изменения, сохраняя, как правило, возможность просмотра объекта.

5. Физическая целостность данных.

Сохранность данных, накопленных в процессе деятельности компании, обеспечивается средствами копирования и восстановления информационной базы. С помощью механизмов планирования и выполнения фоновых заданий могут управляться автоматические операции создания резервных копий, а средства мониторинга параметров базы данных обеспечивают постоянный контроль технических аспектов эксплуатации данного продукта.

Примерно так выглядит краткое описание представленного нами продукта. TIME CARD позволит упростить рабочий процесс вашей компании, вести постоянный учет и в то же время это один из способов защитить свои данные от посторонних лиц.

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных.

Помимо систематического применения арсенала средств, описанных выше, необходимо использовать административные и процедурные меры, в частности регулярное изменение паролей пользователей, предотвращение доступа к физическим носителям информации и т.п.