РАЗРАБОТКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирина Балина, Станислав Панчёхин,
Славянский университет (Республика Молдова)

Problems of maintenance of information safety and system engineering of its protection, various variants of management by access to the information are investigated.

Актуальность выбранной темы обусловлена тем, что защита конфиденциальной и ценной информации от несанкционированного доступа и модификации призвана обеспечить решение одной из наиболее важных задач защиты имущественных прав владельцев и пользователей компьютеров, защиту собственности, воплощенную в обрабатываемой информации от всевозможных вторжений и хищений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб [1, 2].

Целью являлось исследование проблемы обеспечения информационной безопасности (ИБ) компании и разработка системы её защиты. **Новизна** работы определяется тем, что внедрению процедур и норм по обеспечению безопасности информационных процессов на предприятии будет способствовать разработанная База данных (БД) организации доступа к конфиденциальной информации сотрудников (Рис. 1), в которой каждый уровень доступа распознаётся как учетная запись и ей заданы соответствующие настройки безопасности (Рис. 3). Каждому уровню присвоен свой пароль (Рис. 2).

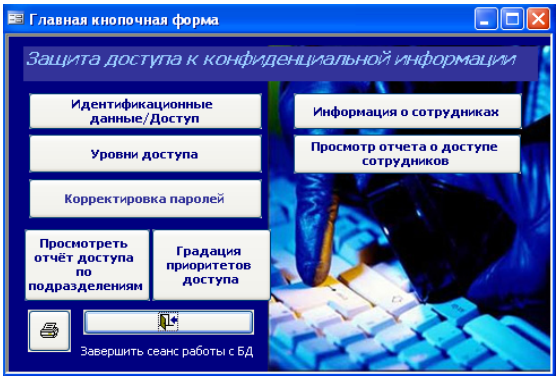
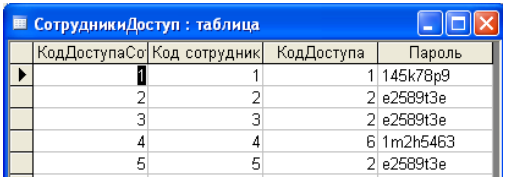


Рис. 1 **Главная форма БД организации доступа к конфиденциальной информации сотрудникам**



СотрудникиДоступ : таблица

КодДоступаСо	Код сотрудник	КодДоступа	Пароль
1	1	1	145k78p9
2	2	2	e2589t3e
3	3	2	e2589t3e
4	4	6	1m2h5463
5	5	2	e2589t3e

***Рис. 2* Таблица «Сотрудники. Доступ» (фрагмент)**

КодДоступа	Описание задачи	Заметки
1	Минимальный	Ограничение доступа пользователей к операциям над документами и справочниками, а также к содержанию (конкретным полям) документов и справочников производится через систему логических рабочих мест
2	Частичный	Возможна работа с конфиденциальными документами по указанию
3	Ограниченный	Доступ к конфиденциальной информации запрещен
...		
7	Повышенные привилегии	Администратор системы контролирует штатные пользовательские командные интерпретаторы, ограничивая возможности пользователя записями в файле "максимальные привилегии".

***Рис.3* Описание ко дов доступа (выборочно)**

Анализ современных технологий зашиты информации позволяет разработать рекомендации по совершенствованию системы безопасности предприятия:

1. Администрирование установок и ограничений работы пользователей: средствами операционной системы, специальных программ и утилит regedit.exe и XP Tweaker- на рабочих станциях (PC) всех сотрудников – прописать учётные записи пользователей, ограничить доступ к дискам и меню задач и др.

2. Постоянный контроль за действиями сотрудников при обработке информации за ПК: контроль в удалённом режиме работы за PC, запуск приложений, содержимое буфера обмена, сетевые подключения и др.

3. Использование возможностей современных криптографических систем – на сервере головного офиса ежедневное шифрование и обновление логического диска для хранения сводной отчётности фирмы, по требованию – производить шифрование текста и (или) файлов при обмене данными с удалёнными пользователями.

4. Установить разработанную СУБД настроек учётных записей всех сотрудников, имеющих доступ к средствам вычислительной техники. Корректировать настройки по мере увольнения/ приёма на работу новых работников/ изменений в штатном расписании и т.д. Разграничить 7 уровней доступа от минимального до повышенных привилегий.

На основании выполненных исследований можно сделать следующие **выводы**:

I. В области понимания информационной безопасности - на сегодняшний день на рынке отсутствует понимание ИБ как таковой. Обычно ИБ сводится к компьютерной

безопасности. При решении, какие услуги предлагать необходимо провести предварительные маркетинговые исследования и выяснить, на что ориентироваться [4].

II. Следствием низкого уровня развития информационных технологий является отсутствие обеспечения информационной безопасности бизнеса. Это приводит к тому, что большинство фирм являются потенциальными целями для умышленного постороннего вмешательства в их нормальную деятельность, со всеми вытекающими отсюда последствиями.

III. При организации работ по совершенствованию информационной безопасности необходим анализ клиентской базы - при внедрении на молдавский рынок услуг, связанных с информационной безопасностью, необходимо четко представлять, на какой круг потребителей можно ориентироваться.

IV. Одним из основных требований к формируемой системе управления безопасностью сетей является то, что данная система должна быть практически действующей и способной выявлять возможные события безопасности, разрабатывать своевременные мероприятия по снижению угроз уничтожения важной информации и выводу из работы системы в целом, вероятности наступления сбоев в работе информационных технологий, рисковых событий или минимизации последствий [3].

V. При внедрении разработанных неформальных (программно- аппаратных) мер защиты по обеспечению информационной безопасности предприятия следует помнить, что они должны быть совмещены с физическими (препятствие – ограничение доступа на предприятие) и с формальными средствами. К ним можно отнести: организационные (регламентация работы сотрудников), законодательные (принуждение в соответствии с законодательством РМ, Международными соглашениями) и морально – этические средства защиты информации (побуждение).

Литература:

1. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. - М.: Академия, 2006.-240с.
2. Клейменов С.А., Мельников В.П., Петраков А.М. Информационная безопасность и защита информации. - М.: Академия, 2008.-336с.
3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. М.: Феникс, 2008.-173с.
4. Балина И.В. Международные аспекты защиты информации в экономических информационных системах. // Тр. Межд. научно-практ. конф. «Экономические аспекты развития современного общества». К.: УЛИМ, 2008, стр. 56 – 62