УДК 004.056

В.В. Федько, А.И. Боднар

Харьковский национальный экономический университет, Харьков

ПОСТРОЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОГРАММАХ СКЛАДСКОГО УЧЕТА

Проводится анализ основных информационных рисков при использовании, разработке и внедрение программ складского учета. Рассматриваются основные способы защиты от утечек информации при использование программ складского учета. Анализируется целесообразность построения комплексной системы информационной безопасности на различных этапах разработки программ для складского учета. Рассматривается построение системы информационной безопасности на примере программы складского учета для оптовой торговли.

Ключевые слова: *информационная безопасность, информационный риск, складской учет, утечка информации.*

Введение

Проблема информационной безопасности возникла с появлением средств информационных коммуникаций, а также с осознанием наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путём воздействия на средства информационных коммуникаций, функционирование и развитие которых обеспечивает информационный обмен между всеми элементами социума.

Основными исследователями в области информационной безопасности на территории СНГ в последние 5 – 7 лет были Щербаков А.Ю., Петренко С.А., Галатенко В.А. Наработки Петренко С.А., представленные в работе «Управление информационными рисками», были использованы для оценки информационных рисков в сфере складского учета в рамках данной статьи.

Основной материал

Важность информации, относящейся к бизнесу трудно переоценить. Пользуясь собранной и обработанной информацией, можно успешно конкурировать на своем рынке и захватывать новые. Информация помогает в поиске партнеров и способствует четкому определению позиции по отношению к ним.

Вопросы безопасности – важная часть концепции внедрения новых информационных технологий во все сферы жизни общества. Увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости

В сфере складского учета фигурируют большие массивы данных, и их утечка может предоставить

конкурентам много важной информации о вашей деятельности. Необходимость постоянного обновления данных для эффективного мониторинга складских остатков, частое добавление новых позиций и товаров увеличивают количество обращений к данным, а следовательно повышают их уязвимость.

В большинстве приложений для автоматизации складского учета содержится множество различной конфиденциальной информации. Последствия от утечки данной информации могут вызвать значительное снижение конкурентной способности фирмы. Особенно это относится к торговым складам. Ведь кроме информации о движении товаров и клиентской базы в системах складского учета для торговли содержатся договора и спецификации, как с поставщиками, так и с клиентами (рис. 1).

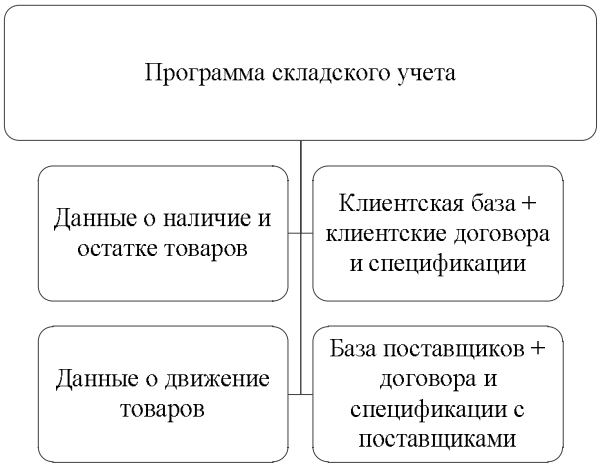

Рис. 1. Основная информация, содержащаяся в программах для складского учета

Если в руки конкурентов попадет информация о движении товаров и список клиентов, они смогут не только усилить свои позиции на рынке, но и использовать наработанный опыт для занятия рыночной ниши. Риск утечки данной информации минимален, поскольку представляет собой лишь сведения о деятельности фирмы, а не механизмы. Сложнее обстоят дела с договорами и спецификациями. Спецификации клиентов и поставщиков следует рассматривать отдельно, т.к. они обладают разной степенью конфиденциальности, и, следовательно, риски при их утечке сильно отличаются.

Клиентские спецификации содержат конкретные цены и скидки для определенного клиента. Их утечка может быть полезна конкурентам для укрепления своих позиций на рынке. С другой стороны, обнародование данных спецификаций может вызвать недовольство у других клиентов относительно собственных закупочных цен и скидок. Это, в свою очередь, приведет к уменьшению клиентской базы, а, следовательно, и прибыли.

Спецификации с поставщиками являются наиболее конфиденциальной информацией в системах складского учета. Они содержат цены, разглашение которых недопустимо как для владельцев склада, так и поставщиков. Риск утечки данной информации наиболее высок. На основе данных спецификаций строится вся документация, в том числе и договоры с клиентами. Данная информация представляет собой механизм деятельности и ее защите нужно уделить наибольшее внимание.

Немаловажным вопросом в безопасности систем складского учета является архитектура приложения. Большинство систем в наши дни имеют сетевую архитектуру для мониторинга сразу нескольких складов. Сеть значительно ускоряет движение данных внутри системы, позволяет отслеживать движение товара сразу по нескольким складам в реальном времени, но с точки зрения информационной безопасности несет в себе множество дополнительных угроз. Автономные решения систем складского учета встречаются все реже и реже, но следует помнить, что даже если система работает локально, компьютер все равно подключен к сети Интернет, что не исключает утечки информации.

Не каждый владелец фирмы знает, как легко можно скопировать его бизнес, потому и не задумывается о безопасности своей информационной системы и начинает принимать меры только после того, как утечка уже произошла [4].

При разработке системы складского учета акцент делается непосредственно на безопасность программного решения, ведь разработчик не несет ответственности за несанкционированные действия пользователей программы, но программисту нужно сделать так, чтобы возможность таких несанкционированных действий была минимальной.

В системах складского учета каналы утечки информации, в основном связанны с доступом к элементам системы и изменением структуры ее компонентов. Если система имеет сетевую структуру, то каналы утечки базируются на несанкционированном доступе и возможно хищение всех данных или их части. Попытки получения информации в таких случаях, как правило, осуществляется удаленно. Это касается и автономных систем, ведь с развитием Интернета становится возможной передача значительных объёмов данных из программ, которые даже не используют сетевую архитектуру. При этом используются либо слабости операционной системы, либо языка программирования, на котором написана программа [2].

Также утечки информации могут быть вызваны пользователями системы. Пользователи системы могут:

1) вести наблюдение за информацией с целью ее запоминания в процессе обработки;

2) осуществлять хищение носителей информации, сбор производственных отходов, содержащих обрабатываемую информацию;

3) преднамеренное считывание данных из файлов других пользователей; чтение остаточной информации, т.е. данных, остающихся на носителях после выполнения заданий;

4) копирование носителей информации;

5) преднамеренное использование для доступа к информации терминалов зарегистрированных пользователей;

6) маскировка под зарегистрированного пользователя путем похищения паролей и других реквизитов разграничения доступа к информации, используемой в системах обработки [3,7].

Следующий вопрос в информационной безопасности систем складского учета – это обеспечение целостности данных. Защита от случайного удаления легко реализуется путем установки систем резервного копирования и настройки прав доступа. Здесь возможна следующая проблема: нет никакой гарантии, что данные удастся восстановить на состояние их удаления. Как правило, резервирование выполняется не чаще чем раз в сутки, а то и неделю. Чем интенсивнее поток товаров проходящих через склад, тем чаще необходимо делать резервное копирование. Однако при частом копировании возникает опасность перехвата всей базы в обход встроенным средствам защиты. Представляется более целесообразным хранить резервные копии на компьютере вместе с программой. Но если система складского учета имеет сетевую структуру и там функционируют большие объемы данных, базы хранятся на отдельном сервере. В случае удаленного хранения данных, необходимо обеспечивать как защиту сервера, так и транзакций. Для защиты транзакций в данном случае достаточно даже простого алгоритма криптования [1].

Реализация периодической смены ролей в системе складского учета, устраняет угрозы несанкционированного доступа к базе складских операций на фирме, а также данных до уровня записи или элемента. Ограничить доступ к информации позволяет совокупность следующих способов:

– иерархическая классификация доступа;

– классификация информации по важности и месту ее возникновения;

– указание специфических ограничений и применение их к специфическим объектам (например, пользователь может осуществлять только чтение файла без права записи в него);

– содержание данных или отдельных групп данных (запрещается читать информацию по отдельным объектам);

– процедуры, представленные только конкретным пользователям. Пользователи программы должны ограничиваться только одной или всеми привилегиями: чтением, записью, удалением информации.

Рассмотрим разграничение ролей на конкретном примере. Ниже приведена структура БД приложения для управления небольшим торговым складом (рис. 2). Программа взаимодействует с двумя пользователями: владелец склада и кладовщик. Владелец добавляет новые товары, вводит цены от поставщи-ков, занимается списком клиентов и ценообразование для каждого из них. Кладовщик занимается отгрузками и составлением учетно-расчетной документации.

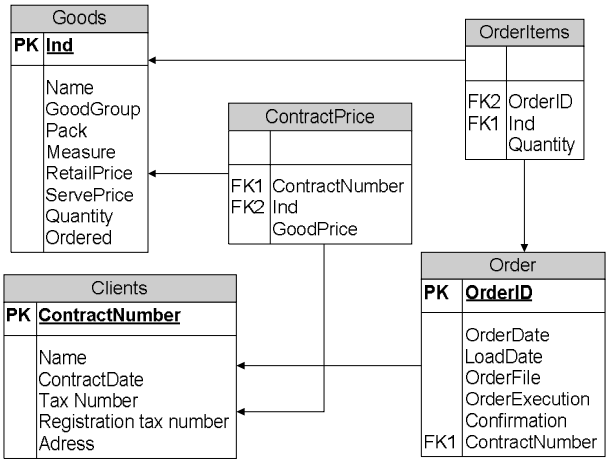

Рис. 2. Структура БД системы складского учета

Для работы обоих пользователей нужен справочник товаров (Goods). Кладовщик использует его для заполнения информации об отгрузке. При этом уровень доступа к данной таблице у кладовщика должен значительно ограничиваться. Ему не разрешено иметь никакого доступа к полям закупочная и отпускная цена (RetailPrice и ServePrice). Также у кладовщика ограничиваются права на редактирование списка клиентов (Clients) и договорных цен (Contact Price). Кладовщик может их просматривать, но не редактировать. Таблицы, связанные с заказами и отгрузками (Orders) полностью доступны для обоих пользователей. Разграничение прав осуществляется посредством учетной записи с паролем, а криптование всей базы служит для предотвращения ее полного хищения.

Сформировав базу возможных рисков, с количественными и качественными индикаторами ущерба и возможностями управления угрозами, перед фирмой возникает другой вопрос: насколько целесообразно защищаться абсолютно от всех возможных угроз? Чтобы ответить на него, необходимо определить перечень наиболее важных. Затем следует приступить к их минимизации. Для определения такой границы критически важно понять суть угрозы, комплексно проанализировать возможный инцидент [5].

Наиболее острым стоит вопрос сетевой безопасности. Даже если решение для складского учета имеет автономную архитектуру, не следует пренебрегать угрозами из Интернета. Чтобы понизить риски возможных сетевых утечек нужно обязательно использовать фаервол на компьютере с системой складского учета. Он позволит контролировать сетевую активность приложения и снизить практически к нулю риск сетевой утечки информации. В наши дни на рынке существуют множество решений в данном сегменте: от стандартного фаервола Windows до сложных программно-аппаратных систем.

Внедрение и обслуживание среднего коммерческого фаервола обойдется около 200 – 250$ в год. Это достойная цена за минимизацию рисков сетевой утечки информации. Если масштабы бизнеса не позволяют приобрести платное программное обеспече-

ние, можно воспользоваться бесплатным. Минимальность рисков при этом будет хуже на 30 – 40%.

Для систем складского учета с сетевой архитектурой необходимо использовать внутреннее криптование данных. Лучше внедрять его еще на этапе разработки программного обеспечения, т.к. потом сделать это будет намного сложнее и дороже. Использование даже самого простого алгоритма криптования снизит риски перехвата транзакций и при резервном копировании. Данное внедрение обойдется в 5 – 10% надбавки к стоимости во время проектировки программного обеспечения и в 20 – 30% для установки алгоритма криптования на систему находящуюся в эксплуатации.

При разработке концепции защиты системы складского учета необходимо исходить из детального анализа направлений деятельности фирмы и комплексных требований защиты. Учитывая многообразие потенциальных угроз информации в системе обработки данных, сложность структуры и функций, а также участие человека в технологическом процессе обработки информации, цели защиты информации систем складского учета могут быть достигнуты только путем создания системы защиты информации на основе комплексного подхода. И начинать создание системы надо с оценки угроз безопасности деятельности коммерческого объекта, а исходя из полученных результатов анализа, принимается решение о построении всей системы защиты и выбираются необходимые средства. Получить достоверную информацию о деятельности фирмы незаконным путем маловероятно, если фирма с пониманием относится к сохранности коммерческой тайны и создания соответствующей системы защиты. В то же время многие под безопасностью понимают, прежде всего, физическую защищенность, иногда включая отдельные требования информационной защиты коммерческих интересов, что не способствует решению проблем безопасности в комплексе.

Выводы

Комплексный организационный подход, эффективный анализ, оценка рисков – залог построения безопасной информационной среды складского учета. Процесс этот непрерывный. От эффективного его внедрения во многом зависит успех бизнеса. Поэтому применение методов системного анализа является важным фактором устойчивости организации.

После анализа рисков утечки информации в системах складского учета можно сделать вывод, что наиболее защищенным модулем в программах складского учета должен быть модуль, содержащий договора и спецификации. Риски утечки остальной информации являются сравнительно незначительными. Для обеспечения информационной безопасности будет достаточным наличие распределения пользователей внутри системы складского учета, а для уверенности можно использовать алгоритмы криптования в тех таблицах БД, где содержится информация о договорах и спецификациях. Для обеспечения сетевой безопасности нужно ограничивать входящие и исходящие сетевые соединения приложения при помощи фаервола, а также блокировать для программы все порты, кроме тех, через которые осуществляется обмен данными с БД.

Список литературы

1. Кузнецов О.О. Захист інформації та економічна безпека підприємства: монографія / О.О. Кузнецов, С.П. Євсеєв, С.В. Кавун. – Х.: Вид. ХНЕУ, 2008. – 360 с.

2. Конхейм А.Г. Основы криптографии / А.Г. Конхейм. – М.: Радио и связь, 1997.

3. Ухлинов А.М. Управление безопасностью информации в автоматизированных системах / А.М. Ухлинов. – М.: МИФИ, 2006.

4. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика, 2007.

5. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.

6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК Пресс, 2008.

7. Петренко С.А. Управление информационными рисками / С.А. Петренко. – М.: Компания АйТи; ДМК Пресс, 2004.

8. [Электронный ресурс]. – Режим доступа к ресурсу: http://infeco.megabyet.net/ - портал информационной безопасности ES INFECO. INTERNATIONAL RESEARCH PORTAL OF INFORMATION AND ECONOMIC SECURITY.

Поступила в редколлегию 1.04.2011

Рецензент: д-р техн. наук, проф. Е.П. Путятин, Харьковский национальный университет радиоэлектроники, Харьков.

ПОБУДОВА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРОГРАМАХ СКЛАДСЬКОГО ОБЛІКУ

В.В. Федько, О.І. Боднар

Проводиться аналіз основних інформаційних ризиків при використанні, розробці та впровадження програм складського обліку. Розглядаються основні способи захисту від втрави інформації при використання програм складського обліку. Аналізується доцільність побудови комплексної системи інформаційної безпеки на різних етапах розробки програм для складського обліку. Розглядається побудова системи інформаційної безпеки на прикладі програми складського обліку для оптової торгівлі.

***Ключові слова**: Інформаційна безпека, складський облік, інформаційний ризик, втрата інформації.*

BUILDING A SYSTEM OF INFORMATION SECURITY IN WAREHOUSE AUTOMATION PROGRAMS

V.V. Fedko, A.I. Bodnar

The analysis of the basic information risks in the use, development and implementation of warehouse management software. The main ways to protect against leaks when using the inventory accounting. Analyzed the feasibility of constructing an integrated system of information security at various stages of development programs for inventory control. The construction of a data security system as an example of inventory control software for the wholesale trade.

***Keywords**: information security, information risk, inventory control, information leakage.*