

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5:658.78

Лабкович
Александр Геннадьевич

Методы обеспечения безопасности
программных приложений для складского учета

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты,
информационная безопасность

Научный руководитель
Шахлевич Григорий Михайлович
к. т. н., доцент

Минск 2018

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.

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

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Для защиты информации в современном автоматизированном складском хозяйстве целесообразно использовать проверенные программные решения, например, решения SAP. Эти решения постоянно обновляются поставщиками систем SAP по мере обнаружения уязвимостей в них.

Однако решения SAP стоят очень дорого, и для снижения издержек производства в складском хозяйстве многие белорусские предприятия экономят на складе. На таких предприятиях эконом-класса ПО для склада не закупается в составе дорогих систем SAP, а разрабатывается самостоятельно силами малочисленного собственного подразделения программистов предприятия. Результатом такой разработки часто является некачественный код, который становится уязвимым для злоумышленников. В этих условиях целью настоящей работы является повышение информационной безопасности программного обеспечения складского хозяйства предприятия эконом-класса путём корректировки программного кода работником склада.

Для достижения поставленной цели в этой диссертации поставлены и решены следующие задачи:

- проведен анализ угроз информационной безопасности на компьютеризированном складе, вызванных некачественным программным кодом.;

- разработаны фрагменты кода (скрипты), позволяющие исправить некачественный код.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выбранной темы, дается краткая характеристика её разработанности, определяется объект и предмет исследования, цель и задачи.

Первая глава «Современный компьютеризированный склад как объект исследования его информационной безопасности» носит теоритический характер и состоит из трех подразделов.

В подразделах 1.1 «Кратко о складском хозяйстве» и 1.2 «Система управления складом как информационный объект» рассматривается суть складского учета и необходимость использования решений SAP для управления складами. SAP-системы - это полезный нужный инструментарий, который существенно облегчает взаимодействие между управляемыми и управляющими структурами в любом бизнесе, особенно крупном и сложно организованном. С их помощью можно обмениваться сведениями с партнерами, интегрировать новые условия и решения с уже существующими. Основные достоинства данной системы:

- сокращение затрат — складских, трудовых (учет/контроль персонала), на капстроительство и прочих;

- ускорение циклов закупки и оборачиваемости по задолженностям;

- упрощение работы бухгалтерии, прочих отделов;

- полноценная локализация;

- возможность объединять с решениями сторонних разработчиков;

- наличие решений для мобильного бизнеса.

В подразделе 1.3 описаны краткие выводы по первой главе.

Во второй главе «Анализ угроз информационной безопасности на складе» проводится анализ основных информационных рисков при использовании, разработке и внедрение программ складского учета. Рассматриваются основные способы защиты от утечек информации при использовании программ складского учета. Анализируется целесообразность

построения комплексной системы информационной безопасности на различных этапах разработки программ для складского учета. Данная глава содержит 5 подразделов. В которых детально описаны основные уязвимости программного кода.

В третьей главе «Методы парирования угроз на компьютеризированном складе финансово устойчивого предприятия» рассматривается наиболее совершенный способ поиска уязвимостей, это статический анализ потока данных. Под статическим подразумевают анализ, осуществляемый с помощью автоматизированных инструментов исходного или исполняемого кода. Такой анализ именуют «Тестирование по методу белого ящика».

Рассмотрены основные программные средства для проведения данного тестирования:

- PolySpace Verifier;
- Coverity Prevent;
- Klocwork K7.

В главе 4 «Методы парирования угроз на компьютеризированном складе эконом-предприятия» описаны способы повышения информационной безопасности программного обеспечения складского хозяйства предприятия эконом-класса путём корректировки программного кода работником склада.

ЗАКЛЮЧЕНИЕ

Тенденции развития инфраструктуры компаний в последнее время движутся от децентрализованной модели к интеграции всех бизнес-процессов в единые системы. В бизнес-приложениях и в ERP-системах хранятся все критичные данные компании, начиная от финансовой отчетности и персональных данных, и заканчивая списками контрагентов и объектами корпоративной тайны. Для внешнего злоумышленника или инсайдера такая система представляет собой основную мишень, и его конечная цель – это отнюдь не права администратора на контроллере домена.

Тем не менее, сейчас многие специалисты по безопасности, к сожалению, крайне поверхностно осведомлены о защите таких бизнес-приложений, как SAP. Проблема также состоит в том, что функции обеспечения безопасности лежат не на CISO, а на владельцах системы, которые фактически контролируют сами себя. В итоге за безопасность наиболее критичных элементов системы никто не отвечает.

Решения SAP стоят очень дорого, и для снижения издержек производства в складском хозяйстве многие белорусские предприятия экономят на складе. На таких предприятиях эконом-класса ПО для склада не закупается в составе дорогих систем SAP, а разрабатывается самостоятельно силами малочисленного собственного подразделения программистов предприятия. Результатом такой разработки часто является некачественный код, который становится уязвимым для злоумышленников.

Применение методов системного анализа является важным фактором устойчивости организации.

В данной работе проводится анализ основных информационных рисков при использовании, разработке и внедрение программ складского учета. Рассматриваются основные способы защиты от утечек информации при использовании 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.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

- Лабкович, А. Г. Особенности автоматизации управления складом готовой продукции в аспекте его информационной безопасности // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 51–57.

- Лабкович, А. Г. Скрипты, позволяющие исправить некачественный код на складе готовой продукции предприятия эконом-класса с целью повышения информационной безопасности складского ПО // в печати.