УДК 004.041

д.т.н., проф. **Бойченко О.В.** (Тавр.НУ)
Тупота Е.С. (Тавр.НУ)

МЕТОД КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ НА ОСНОВЕ CRM-СИСТЕМ

В статье предложено применение CRM-систем на предприятии для выявления определения внешних вмешательств, утечки корпоративной информации, систематизацию хранения клиентской базы предприятия экономического предприятия.

Проведено исследование жизненного цикла методов реагирования на вмешательства в систему извне.

Установлено, что для поддержания системы необходимо внедрять дополнительный уровень защиты, который мог бы обеспечить отказоустойчивость системы в целом. Полученные результаты доказывают актуальность использования данного класса систем и необходимость внедрения дополнительного уровня защиты.

Ключевые слова: информационная система поддержки решений, ситуационный центр, информационная система, хранилище данных, CRM-система.

Постановка проблемы. Современный этап развития бизнеса характеризуется широким использованием средств автоматизации процессов внутри управляющей системы. Это обусловлено необходимостью постоянного контроля процесса взаимоотношений клиента и предприятия, обеспечивающего создание условий для повышения эффективности работы отделов. Целью работы является исследование CRM систем, выявление уровней защиты обеспечивающих сохранность и отказоустойчивость системы.

Изложение основного материала. В настоящее время для решения указанных проблем необходимо внедрять Системы управления взаимоотношениями с клиентами, далее CRM-система, представляющие собой программное обеспечение, направленное на автоматизацию процесса взаимодействия с клиентами. Внедрение CRM-систем позволяет создавать общую базу контактов предприятия, осуществлять непосредственный контроль эффективности работы отдела продаж, получать своевременную аналитическую и статистическую информацию, планировать стратегию развития предприятия, предпринимать своевременные управленческие решения. Кроме того, внедрение облачные сервисов позволяет экономить бюджет предприятия, так как традиционное решение является дороже в процессе внедрения и поддержки управляющих информационных систем.

Однако проблемой внедрения облачных технологий является обеспечение надежной защиты данных, что обусловлено широкими возможностями несанкционированного доступа к клиентской базе предприятия и документам компании по причине открытости CRM-системы [1].

В качестве решения указанной проблемы может быть предложена технология многоуровневой защиты данных компании, использующей CRM-системы.

Первым является уровень физической защиты, основанный на обеспечении круглосуточной охраны датацентров, а также обеспечением сохранности информации, хранящуюся на серверах средствами резервного копирования. Так же относится обеспечение защиты мобильных каналов связи сотрудников центра.

Защита информации на уровне передачи данных представляет второй уровень, основанный на использовании уровня защищенных сокетов (SSL) – сертификата, который уникальным способом идентифицирует пользователей и различные сервера. Это обеспечивает создание зашифрованного канала безопасной передачи данных.

Третий уровень обеспечивает авторизацию в системе, позволяющую автоматически определять наличие доступа к конкретному отделу базы данных путем осуществления

контроля логина и пароля пользователя при загрузке новой страницы и изменении критической информации.

Четвертый уровень обеспечивает определение позиционирования операций в системе как отдельного объекта доступа с определением прав для отдельных пользователей и распределения доступа к документообороту.

Пятый уровень организует контроль безопасности путем фиксации в системном журнале любого доступа к данным.

Таким образом, использование многоуровневой системы защиты информации в CRM технологиях обеспечивает эффективную защиту коммерческой информации компании от несанкционированного доступа наряду с открытым доступом к данным, необходимым для сотрудников фирмы [2].

Анализ практического опыта использования многоуровневой системы защиты данных на основе CRM-технологии позволил сделать предположение о возможности введения в ее состав нового уровня защиты информации (уровня реагирования), с целью создания условий для реакции информационной системы на несанкционированные влияния и контроля целостности данных [3].

В основе работы уровня реагирования (базового в отношении разрабатываемой модели) лежит метод сценариев реагирования на события в сфере безопасности для обеспечения гарантированного оперативного и корректного реагирования на атаку. Прогноз указывает, что внедрение метода сценариев может обеспечить повышение уровня восстанавливаемости работоспособности информационной системы до 20%.

Основой разработанной методики являются 7 этапов в соответствие со стандартной процедурой жизненного цикла информационной системы (рис. 1).

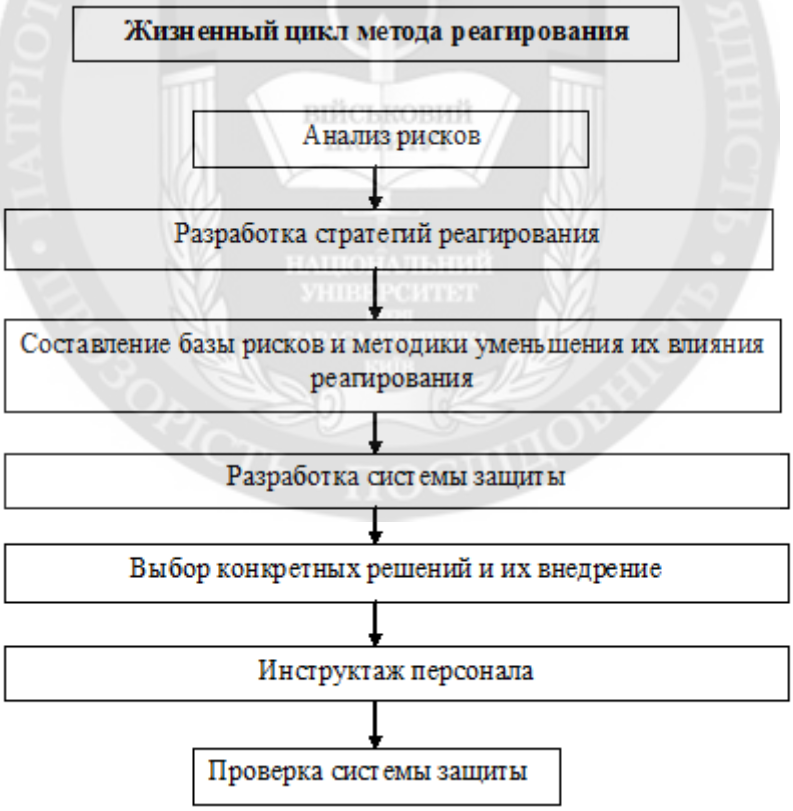

Рис. 1. Жизненный цикл метода реагирования (контроля целостности данных)

На этапе анализа рисков обеспечивается качественная оценка риска (субъективная для каждого предприятия), что минимизирует отсутствие достоверных статистических данных о вероятности реализации определенной атаки на информационные ресурсы предприятия. Так же стоит учесть, что данная оценка является.

Подробный анализ рисков позволяет рассмотреть предприятие в виде структурной схемы в составе информационных потоков с ранжированием ресурсов, что позволяет провести оценку уязвимостей, связанных с информационными потоками и их утечками.

Кроме того, на данном этапе осуществляется документирование компьютерной системы предприятия, что позволяет создавать условия для выявления критических приложений с указанием источника возможных ошибок. В последующем это обеспечивает выявление и документирование уязвимостей компьютерной системы в системе ранжирования рисков.

Стоит отметить, что присвоение определенных значений и вероятностей осуществления события взлома накладывает определенный след на модель, так как в дальнейшем оценка корректности разработанного метода базируется на основе этих данных, являющихся сугубо субъективными. Однако, благодаря метрическим оценкам защищенности данных системы, становится возможным первично определить условия и приоритеты для построения модели защиты информационной системы.

Этап разработки стратегий реагирования основан на предыдущих исследованиях и направлен на построение модели реагирования. Такая модель обеспечивает осуществление грамотного распределения бюджетных средств и дальнейшее осуществление приоритетной разработки стратегий.

Отличием данного этапа является разработка модели нарушителя, которая представляет собой описание видов взломщиков, преднамеренно (непреднамеренно) осуществляющих взлом информационной системы. Методика включает последовательное распределение злоумышленников на внутренних и внешних взломщиков, а также их более конкретную типизацию. Так, к категории внешних злоумышленников относятся клиенты, наносящие ущерб преднамеренно (непреднамеренно), подрядчики, хакеры, ремонтники и т.д., а в свою очередь внутренними злоумышленниками являются сотрудники, осуществляющие взлом преднамеренно (непреднамеренно) в зависимости от уровня доступа.

Это позволяет создать условия гибкости приоритетов стратегий реагирования на основе 3-5 уровня защиты CRM-технологии.

На этапе составление базы рисков и методики уменьшения их влияния осуществляется выявление ключевых рисков, связанных с системой в целом и некоторыми ее отдельными элементами.

На данном этапе существуют несколько ключевых промежуточных этапов:

– оценка всевозможных рисков, связанных с эксплуатацией компьютерной системы в целом;

– оценка и выявление угроз, связанных с реализацией атак на выявленных уязвимостях;

– оценка степени защиты компьютерных узлов;

– оценка уровня безопасности хранимых и обрабатываемых данных внутри системы;

– оценка уровня своевременного обеспечения отделов правильной информации, отслеживание некорректных потоков информации;

– детальная разработка документации, описывающей компьютерную систему предприятия;

– выявление слабо защищенных приложений в реализованной компьютерной системе.

На этапе разработки системы защиты осуществляется разработка сценариев реагирования. При этом, на основе предыдущих этапов, разрабатываются всевозможные сценарии реагирования системы в случае преднамеренного (непреднамеренного). Кроме того, разработка системы защиты учитывает определение угрозы, ее источник, тип и инструменты.

Данный этап можно разделить на следующие под этапы:

– разработка структуры сценариев реагирования;

– физическая реализация;

– программная реализация.

На этапе выбора конкретных решений и их внедрение производится определение всех функциональных требований для снижения рисков и выбор возможных решений для контроля. Наряду с этим проводится проверка адекватности предложенных элементов контроля на соответствия всем функциональным требованиям по реализации защиты, оценка снижения вероятности осуществления внешнего воздействия или вероятность риска, оценка стоимости реализации защиты компонентов и нейтрализации угрозы, риска, а также определение наиболее экономически адекватных решений реализации защиты путем анализа затрат и выгод.

Важным фактором на данном этапе является реализация контроля путем осуществления пробного использования решений для его контроля и пробы эффекта непосредственно на предприятии.

Этап инструктажа персонала призван обеспечить всем сотрудникам предприятия изучение всех аспектов в области информационной безопасности организации с четким освоением всех сценариев реагирования и своевременного принятия решений для реагирования инциденты, связанные с защитой данных. Методика также учитывает дифференциальный подход в обучении, зависящий от уровня распределения прав доступа пользователей [4].

На данном этапе проверки системы защиты осуществляется попытка обнаружений внешних аномалий, воздействующих на сеть, что способствует гарантии удачного внедрения заранее разработанного сценария.

Целью проверки системы защиты является:

– обеспечение дополнительных гарантий в том, что требования, связанные с безопасностью полностью проанализированы и задокументированы;

– исключение дополнительных расходов, связанных с реализацией системы защиты информации;

– исключение субъективной оценки рисков;

– оказание поддержки в планировании и реализации всех стадий сценария реализации;

– обеспечение проведения всевозможных работ в краткие сроки;

– автоматизация процесса анализа требований;

– обоснование мер по защите от внешнего воздействия;

– оценка разработанных сценариев, составление списка условий для реализации того или иного сценария;

– автоматическая генерация отчетности.

Полученные научные результаты. В заключение отметим, что разработкой нового метода реагирования (контроля целостности данных) в системе защиты данных ИС на основе CRM-технологий возможно создание условий для оперативного выявления несанкционированного влияния на систему управления, что обеспечивает повышение уровня восстанавливаемости работоспособности ИС предприятия до 20%.

Выводы. Разработанный метод является гибким во внедрении с учетом обязательной корректировки в случае изменений в структуре системы, внедрения новых технологий, введения новых серверов в эксплуатацию, создания нового клиента (приложение, новый веб-ресурс), а также в случае изменений в порядке осуществления деятельности предприятия.

ЛИТЕРАТУРА:

1. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М: Госстандарт России, 2002.

2. Защита клиентской базы предприятия при использовании CRM-систем / О.В. Бойченко, Е.С. Тупота // Актуальные проблемы и перспективы развития экономики: XIV Междунар. науч.-технич. конф., 12-14 ноября 2015 г.: тезисы докладов. – Симферополь, 2015. – С. 240-241.

3. Международный стандарт ISO/IEC 27001:2013 “Системы менеджмента информационной безопасности”, 25.09.2013. – Электронный ресурс [Режим доступа]. - rusregister.ru/press-center/.

4. Руководство по управлению рисками безопасности. Группа разработки решений Майкрософт по безопасности и соответствию регулятивным нормам и Центр Microsoft security center of excellence. – URL: http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/

5. Серебряник И. А., Федорова С. В. Управление взаимоотношениями с клиентами: применение CRM-систем // Актуальные проблемы гуманитарных и естественных наук. 2012. №1.С.53-55

6. Лучникова Е. В., Коновалов С. В., Чекал Е. Г. Концепции защиты данных в системе единого реестра инфокоммуникационных услуг // Перспективы развития информационных технологий. 2012. №8. С.136-140.

7. Шимон Николай Степанович Способы и средства защиты от сетевых атак в Единой информационно-телекоммуникационной системе органов внутренних дел // Вестник ВИ МВД России. 2009. №1. С.164-167.

8. Buttle, F. (2003). Customer Relationship Management - Concept and Tools, Elsevier: Boston.

REFERENCES:

1. GOST R ISO/MJeK 15408-1-2002. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast' 1. Vvedenie i obshhaja model'. – M: Gosstandart Rossii, 2002.

2. Zashhita klientskoj bazy predprijatija pri ispol'zovanii CRM-sistem / O.V. Bojchenko, E.S. Tupota // Aktual'nye problemy i perspektivy razvitija jekonomiki: XIV Mezhdunar. nauch.-tehnich. konf., 12-14 nojabrja 2015 g.: tezisy dokladov. – Simferopol', 2015. – S. 240-241.

3. Mezhdunarodnyj standart ISO/IEC 27001:2013 “Sistemy menedzhmenta informacionnoj bezopasnosti”, 25.09.2013. – Jelektronnyj resurs [Rezhim dostupa]. - rusregister.ru/press-center/.

4. Rukovodstvo po upravleniju riskami bezopasnosti. Gruppa razrabotki reshenij Majkrosoft po bezopasnosti i sootvetstviju reguljativnym normam i Centr Microsoft security center of excellence. – URL: http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/

5. Serebrjanik I. A., Fedorova S. V. Upravlenie vzaimootnoshenijami s klientami: primenenie CRM-sistem // Aktual'nye problemy gumanitarnyh i estestvennyh nauk. 2012. №1.C.53-55

6. Luchnikova E. V., Konovalov S. V., Chekal E. G. Koncepcii zashhity dannyh v sisteme edinogo reestra infokommunikacionnyh uslug // Perspektivy razvitija informacionnyh tehnologij. 2012. №8. S.136-140.

7. Shimon Nikolaj Stepanovich Sposoby i sredstva zashhity ot setevyh atak v Edinoj informacionno-telekommunikacionnoj sisteme organov vnutrennih del // Vestnik VI MVD Rossii. 2009. №1. S.164-167.

8. Buttle, F. (2003). Customer Relationship Management - Concept and Tools, Elsevier: Boston.

Без рецензії.

д.т.н., проф. Бойченко О.В., Тупота О.С.

МЕТОД КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ НА ОСНОВЕ CRM-СИСТЕМ

У статті запропоновано застосування CRM-систем на підприємстві для виявлення визначення зовнішніх втручань, витоку корпоративної інформації, систематизацію зберігання клієнтської бази підприємства економічного підприємства.

Проведено дослідження життєвого циклу методів реагування на втручання в систему ззовні.

Встановлено, що для підтримки системи необхідно впроваджувати додатковий рівень захисту, який міг би забезпечити відмовостійкість системи в цілому. Отримані результати доводять актуальність використання даного класу систем і необхідність впровадження додаткового рівня захисту.

Ключові слова: інформаційна система підтримки прийняття рішень, ситуаційний центр, інформаційна система, сховище даних, CRM-система.

Prof. Boychenko O.V., Tupota E.S.

RESPONSE METHOD IN PROTECTION DATA SYSTEMS BASED ON CRM-SYSTEMS

In the article were proposed the use of CRM systems in the enterprise to identify the definition of external interventions, leakage of corporate information, organize storage client base of the company economic enterprises.

A study of the life cycle methods of response to intervention in the system from the outside were proposed.

It is established that for maintenance of the system it is necessary to introduce an additional level of protection that would ensure the resiliency of the system as a whole. The results demonstrate the relevance of the use of this class of systems and the need to implement additional levels of protection.

Keywords: information system decision support, situational center, information system, data warehouse, CRM system.