УДК 681.518.3

МЕТОДИКА МОНИТОРИНГА НАДЕЖНОСТНЫХ ПОКАЗАТЕЛЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В БАНКЕ ПО ДАННЫМ ИХ ТЕКУЩЕЙ ЭКСПЛУАТАЦИИ

С.В. Попов, В.Н. Шамкин

ФГБОУ ВПО «Тамбовский государственный технический университет», г. Тамбов

Рецензент д-р техн. наук, профессор Д.Ю. Муромцев

Ключевые слова и фразы: журнал работы; инцидент информационной безопасности; нарушение работоспособности; показатели надежности; событие информационной безопасности; средство контентного анализа.

Аннотация: Изложена методика, позволяющая по данным текущей эксплуатации, извлекаемым из журналов работы средств защиты информации, расположенных на нижнем уровне системы мониторинга инцидентов информационной безопасности банка, получать администратору регулярно обновляемые сведения, характеризующие надежность как отдельных компонентов этих средств защиты, так и каждого из них в отдельности.

В работах [5–8] рассматривались различные вопросы, связанные с исследованием влияния надежности средств защиты информации (**СЗИ**), входящих в состав системы мониторинга инцидентов информационной безопасности (**СМИИБ**), на эффективность ее функционирования в автоматизированной банковской системе (**АБС**). Необходимость получения администратором безопасности АБС оперативных данных по оценке надежности СЗИ отмечалась в [6]. Значимость этих данных для принятия соответствующих решений администратором и влияние последних на обеспечение информационной и экономической безопасности банка обоснована в статье [7].

В случае выхода из строя одного или нескольких СЗИ, а также в связи с невыполнением ими своих отдельных функций, может быть серьезно

Попов Сергей Викторович – соискатель кафедры «Конструирование радиоэлектронных и микропроцессорных систем», e-mail: posevik@yandex.ru; Шамкин Валерий Николаевич – доктор технических наук, профессор кафедры «Конструирование радиоэлектронных и микропроцессорных систем», e-mail: crems@crems.jesby.tstu.ru, ТамбГТУ, г. Тамбов.

нарушен процесс мониторинга инцидентов информационной безопасности (**МИИБ**) [8]. Во время бездействия или нештатного функционирования какого-либо СЗИ возникает угроза пропуска инцидентов информационной безопасности (**ИИБ**)[1], поскольку это СЗИ не обеспечивает адекватной защиты конфиденциальной информации (**КИ**) банка. Реализация угрозы может снизить эффективность функционирования СМИИБ, а, следовательно, и АБС. В этой связи необходимо скорейшее выявление и устранение причин отказа или нештатного функционирования СЗИ.

Как отмечалось в [6] на нижнем уровне СМИИБ располагаются различные программно-аппаратные СЗИ, собирающие данные о событиях ИБ в АБС: сканер безопасности (**СБ**); антивирусное программное обеспечение (**АПО**); средство контентного анализа (**СКА**); средство контроля портов ввода/вывода (**СКПВВ**); межсетевой экран (**МСЭ**); система обнаружения атак (**СОА**) и др.

Продемонстрируем методические аспекты того, как можно определять характеристики надежности различных СЗИ, используя журналы работы, фиксирующие во времени определенным образом их функционирование
в составе АБС. Такие сведения крайне необходимы администратору безопасности, поскольку они позволят ему снизить уровень неопределенности в процессе принятия решений, так как он будет получать более достоверные данные об истинном состоянии работоспособности средств защиты информации.

Среди СЗИ, с точки зрения надежности, выделим два вида средств: с дискретным и непрерывным временем функционирования. Рассуждения здесь проведем на примере средства контентного анализа (**СКА**), принадлежащего к дискретному виду средств защиты.

Структура и принцип работы СКА

Средство контентного анализа представляет собой программно-аппаратный комплекс, который предназначен для мониторинга сетевого трафика с целью выявления нарушений политики безопасности.

Различные СКА используют разные источники информации, предназначенной для последующего анализа. При этом структура СКА остается практически неизменной, за исключением модуля-посредника, который меняется в зависимости от источника информации. Выделяют несколько видов СКА [7–8]: различные системы аудита – почтовых сообщений, мгновенных сообщений, IP-телефонии, файлов, копируемых на съемные носители; системы мониторинга интернет-трафика и др.

Из многообразия СКА рассмотрим систему аудита файлов, копируемых на съемные носители (на примере ПО DeviceSniffer). Выбор обусловлен тем, что съемные носители представляют наибольшую угрозу безо-

[1] ИИБ – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности (**СИБ**), с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ [1].

СИБ – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [1].

пасности информации, циркулирующей в АБС [3, 9]. В этой системе источником информации, подлежащей последующему контентному анализу, является другое средство ЗИ, а именно, СКПВВ. Такая система аудита используется для сбора информации о выносимых за пределы АБС файлах и для ее последующего анализа с целью выявления файлов, несоответствующих требованиям безопасности банка.

На рисунке 1 представлена структурная схема подобной системы аудита файлов, содержащей источник информации – СКПВВ и, собственно, СКА.

Агенты (программы-агенты) СКПВВ, установленные на автоматизированных рабочих местах (**АРМ**) сотрудников АРМ 1, …, АРМ *N* осуществляют «теневое копирование», то есть перехватывают файлы, скопированные пользователями на различные съемные носители, и передают их через сервер СКПВВ в БД СКПВВ (на рисунке 1 эти процессы отмечены штриховой линией).

Основными активными программными компонентами СКА являются [2]: модуль-посредник, индексирующий сервер и модуль проверки индекса, а хранилище данных (**ХД**) и индекс представляют собой некие структуры данных, необходимые для их функционирования. Активные компоненты выделены на рис. 1 фоном.

Сведения о файлах, полученные в результате теневого копирования, а также их содержимое, модуль-посредник СКА извлекает из БД СКПВВ и записывает их в ХД СКА, настроенное для индексирования. Эти данные обрабатываются при помощи индексирующего сервера, в результате чего получается структура данных, необходимая для быстрого поиска нужной информации в перехваченных файлах. Такая особая структура называется индексом [8]. Индекс опрашивается по списку контрольных слов, выражений и текстовых фрагментов. Для настройки расписания проверок и редактирования списка запросов используется модуль проверки. В случае обнаружения файлов, нарушающих требования безопасности, модуль проверки индекса высылает администратору соответствующее сообщение.

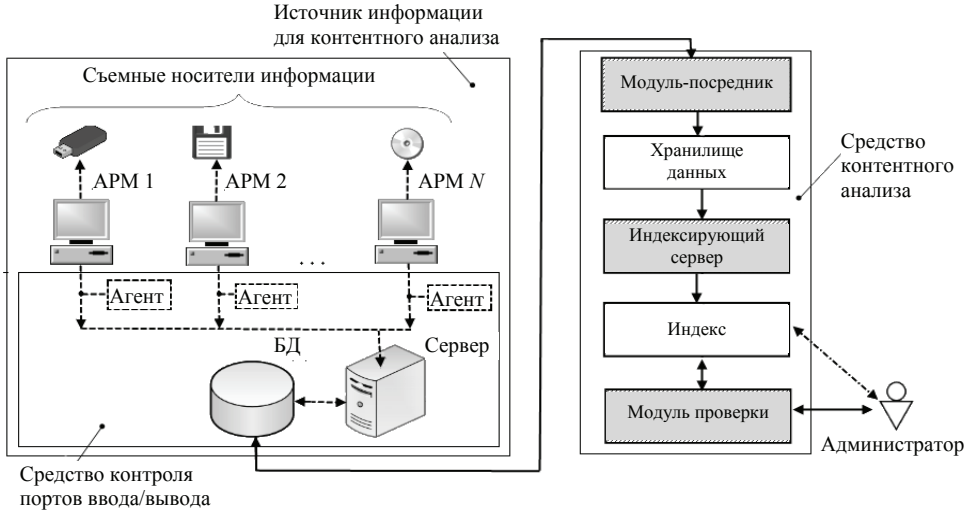

Рис. 1. Структурная схема системы аудита файлов, копируемых на съемные носители информации

Характерной особенностью штатного функционирования СКА является то, что его активные компоненты выполняют свои основные функции периодически, с разной частотой:

– модуль-посредник – функцию копирования файлов из БД СКПВВ в ХД один раз в минуту;

– индексирующий сервер – функцию обновления индекса по расписанию (например, три раза в сутки, – в 7:00, 15:00 и 23:00) и по запросу администратора (по мере необходимости);

– модуль проверки – функцию проверки в режиме, аналогичном работе индексирующего сервера, но с небольшим запаздыванием.

Выявление ошибок функционирования

При нарушениях в работе отдельных программных компонентов СКА, понимаемых нами, как невыполнение ими основных функций, как правило, продолжается выполнение других основных и второстепенных функций СКА. Поэтому для оценки характеристик надежности СКА нельзя применять кажущуюся верной (при взгляде на рис. 1) структурную схему надежности в виде последовательного соединения соответствующих программных компонентов. Очевидно, что исходить в дальнейшем следует из понятия эффективности функционирования СКА (с точки зрения надежности), то есть рассматривать его аналогично [3], как сложную систему на множестве состояний функционирования [6, 7].

Рассматривая СКА как объект исследования на надежность, отдельно следует обратить внимание на такой активный компонент, как модуль проверки индекса. Его основная функция состоит в том, что модуль периодически обращается к индексу СКА с запросом, содержащим список контрольных слов, выражений и текстовых фрагментов, который составлен администратором. При обнаружении фактов несоблюдения политики безопасности модуль проверки передает администратору соответствующее уведомление.

В случае нештатного выполнения модулем этой функции (как показывает практика, весьма редких) администратор может передавать запрос в индекс вручную и получать соответствующие результаты, то есть может на некоторое время взять исполнение функций модуля проверки на себя. На рисунке 1 данное обстоятельство отмечено штрихпунктирной линией. В этой связи представляется целесообразным принять допущение о том, что модуль проверки индекса надежен и постоянно находится в состоянии нормального функционирования.

В соответствии со сказанным, далее будем говорить о выполнении или невыполнении своих основных функций такими активными компонентами СКА, как модуль-посредник и индексирующий сервер.

Оценки показателей надежности активных компонентов СКА определим, проанализировав сведения из журналов работы модуля-посредника и индексирующего сервера СКА, функционировавшего в АБС крупного банка в течение 9 месяцев 2011 г. Эти журналы обычно используются администратором безопасности АБС в своей повседневной работе для просмотра СИБ с целью последующего выявления ИИБ и получения служебной информации, включая и сведения о нарушениях в работе компонентов.

Вообще говоря, по информации, извлекаемой из этих журналов, можно оперативно определять различные характеристики надежности рассматриваемых компонентов СКА, которые впоследствии необходимы при оценке надежности и эффективности функционирования СКА. Имеются в виду интегральные и дифференциальные функции распределения случайных времен работы и восстановления работоспособности компонентов; вероятности и плотности вероятностей их безотказной работы; вероятности отказа и восстановления; интенсивности отказов и восстановлений; числовые характеристики – средние времена работы и восстановления, их дисперсии и т.д.

В журнале модуля-посредника, наряду со служебной информацией: версия операционной системы (**ОС**) сервера, имя подключенной БД СКПВВ, время запуска и остановки модуля, различные сообщения об ошибках и т.п., содержится перечень файлов, добавленных в ХД модулем за анализируемый период времени. В течение девяти месяцев ежедневно в журнал в среднем заносилось $19 \cdot 10^3$ записей, а за весь период наблюдения внесено приблизительно $5{,}059 \cdot 10^6$ записей. Размер файла журнала равен приблизительно 1 Гб.

Журнал индексирующего сервера содержит следующие служебные сведения: о моментах запуска, остановки и перезагрузки сервера; об используемых индексах и моментах их подключения; о количестве проиндексированных файлов в ходе соответствующего обновления индекса; о произошедших ошибках и т.д. Ежедневно в журнал заносилось в среднем 1200 записей, а всего было внесено примерно $3{,}297 \cdot 10^5$ записей. Размер файла журнала работы составил около 40 Мб.

Суммарное число записей в журналах работы индексирующего сервера и модуля-посредника СКА за рассматриваемый период равно $5{,}389 \cdot 10^6$.

Для облегчения поиска записей об ошибках в работе компонентов было предложено использовать информацию о событиях информационной безопасности[2], происходящих в АБС, которую администратор безопасности регулярно получает от СКА в виде сообщений, приходящих по электронной почте.

Пример распечатки полученного администратором сообщения о произошедшем СИБ, заключающемся в копировании файла «Отчет о доходах.txt»:

> **Уведомление № 102** по критерию проверки «Конфиденциально» перехвачено SearchInform DeviceSniffer 03.06.2011 11:05:08 **Пользователь** GO\Ivanov.
> **Компьютер** Ivanov-XP **Размер файла:** 21683220 **Файл:** \\Работа\Отчет_о_ доходах.txt.

[2] Для СКА событие ИБ – выявление скопированных на сменный носитель файлов, содержание которых формально соответствует заданным критериям поиска возможных нарушений политики ИБ банка. Инцидент ИБ – выявление скопированных на сменный носитель файлов, содержание которых соответствует не только заданным формальным, но и дополнительным неформальным критериям.

Модуль проверки СКА включается регулярно в 7:15, 15:15 и 23:15, то есть через каждые 8 ч, и среди поступивших в СКА файлов осуществляет поиск СИБ – файлов, которые соответствуют хотя бы одному из восьми установленных критериев. Среди критериев поиска: наличие в документе слова «конфиденциально»; наличие в документе номеров кредитных карт; копирование файлов-таблиц, превышающих некий установленный размер, и т.п. Соответственно по окончании каждой проверки поступивших в СКА файлов можно получить максимум восемь сообщений (по одному на каждый критерий).

При нормальном функционировании компонентов СКА практически при каждой проверке обнаруживается хотя бы одно СИБ по какому-либо критерию. При этом среднее число СИБ на отдельных интервалах проверки с течением времени значительно не изменяется. Наличие сообщений о подобных событиях, передаваемых администратору безопасности, можно расценивать как признак нормальной работоспособности СКА.

Если один или оба компонента СКА находятся в состоянии отказа или функционируют (в силу различных причин) с пониженной эффективностью, то СКА или полностью, или частично не выполняет своих функций по защите конфиденциальной информации. Это проявляется в том, что СИБ либо совсем не обнаруживаются, либо обнаруживаются, но не в полном объеме. Соответственно часть из них не фиксируется, а значит, данные о них не поступают администратору. Если в результате проверки не обнаруживается ни одного СИБ и администратору не посылается ни одного сообщения, или если количество СИБ на отдельных интервалах проверки (7:15 – 15:15; 15:15 – 23:15; 23:15–7:15) значительно отличается от средних значений, то это можно расценивать как возможное нарушение в работе СКА.

Следует заметить, что в выходные дни, когда количество файлов, копируемых сотрудниками на съемные носители информации, становится, в силу естественных причин, значительно меньше, это не следует считать признаком возможного нарушения работы СКА.

В таблице приведены результаты рассмотрения всех сообщений о СИБ, полученных администратором по электронной почте с января по сентябрь 2011 г., на предмет выявления отрезков времени, в которые сообщения о СИБ не поступали. Из нее видно, что за время рассмотрения было найдено 18 таких отрезков времени, на которых затем анализировалась работа компонентов СКА (индексирующего сервера и модуля-посредника) по журналам с целью выявления фактов нарушения их функционирования. Это позволило весьма значительно сократить объем записей, подлежащих анализу.

Жирным шрифтом в таблице выделены те промежутки времени, на которых действительно были выявлены нарушения. Наиболее часто встречались следующие нарушения, упоминаемые в журналах работы компонентов СКА как ошибки:

1) произошла несанкционированная очистка (обнуление) индекса СКА;

2) отсутствует реакция индексирующего сервера СКА на управляющие воздействия;

Отрезки времени, в течение которых от СКА не поступало сообщений о СИБ

Номера отрезков времени	Дата начала	Время	Дата окончания	Время
1	**19.01.11**	**08:05**	**20.01.11**	**15:10**
2	22.01.11	08:15	24.01.11	15:33
3	29.01.11	08:15	30.01.11	08:00
4	**01.02.11**	**08:15**	**03.02.11**	**17:05**
5	**14.02.11**	**11:25**	**16.02.11**	**07:03**
6	**02.03.11**	**08:15**	**04.03.11**	**08:04**
7	06.03.11	08:10	07.03.11	07:07
8	18.03.11	17:16	19.03.11	07:12
9	05.04.11	14:01	06.04.11	07:03
10	09.04.11	13:10	11.04.11	07:02
11	15.04.11	15:13	16.04.11	11:21
12	30.04.11	14:00	01.05.11	17:45
13	**07.05.11**	**08:15**	**10.05.11**	**14:00**
14	**16.05.11**	**08:05**	**17.05.11**	**07:06**
15	18.05.11	13:14	19.05.11	17:08
16	**16.06.11**	**17:23**	**18.06.11**	**07:12**
17	**30.08.11**	**10:45**	**01.09.11**	**13:15**
18	**18.09.11**	**17:33**	**19.09.11**	**07:08**

3) невозможно осуществить копирование файлов в хранилище данных СКА по причине отсутствия свободного места на жестком диске сервера, на котором установлено СКА;

4) невозможно осуществить копирование файлов в ХД СКА по причине неудачной аутентификации модуля-посредника в БД СКПВВ.

Первые две ошибки относятся к индексирующему серверу, а последние – к модулю-посреднику. По некоторым из таких ошибок СКА сразу автоматически принимает меры по их устранению. Такой, в частности, является первая ошибка. По другим ошибкам требуется обязательное участие администратора, который, несмотря на появляющиеся записи в журналах об ошибках, не всегда может, в силу разных причин, своевременно реагировать на них. Вследствие этого в журналах по некоторым ошибкам могут появляться повторяющиеся до тех пор записи, пока администратор не обнаружит их и не начнет принимать соответствующие меры по устранению ошибок. Таким образом, по одним из ошибок можно считать, что у них имеется только время устранения, а по другим – время поиска и время устранения.

Определение показателей надежности СКА

Записи из журналов работы компонентов СКА о встречающихся нарушениях, их видах и об устранении этих нарушений (автоматически или силами администратора) являются источником данных для последующего определения показателей надежности этих компонентов, а, следовательно, и СКА. Естественно, что таких данных должно быть достаточное количество для того, чтобы можно было определить с допустимой точностью

статистические оценки показателей, то есть выборки должны быть представительными.

Продемонстрируем методику вычисления показателей надежности компонентов СКА.

Траектория изменения во времени состояния функционирования $h(t)$ какого-либо компонента на выбранном интервале наблюдения $[t_0, t_н]$ в связи с появлением ошибки определенного вида может быть представлена, как показано на рис. 2.

Здесь h_0 – состояние работоспособности компонента; h_j – состояние нарушения работоспособности компонента вследствие ошибки *j*-го вида, $j = \overline{1,4}$; t_i^j – момент возникновения *i*-й ошибки ($i = \overline{1,k}$) *j*-го вида, взятый из первой записи об *i*-й ошибке *j*-го вида в журнале; $t_{пi}^j$ – момент обнаружения (поиска) администратором *i*-й ошибки *j*-го вида и начала ее устранения, который взят из последней записи об *i*-й ошибке *j*-го вида; $t_{вi}^j$ – момент окончания устранения *i*-й ошибки *j*-го вида, взятый из записи, характеризующей восстановление работоспособности компонента после *i*-й ошибки *j*-го вида; T_i^j – случайное время работы между *i*-й и (*i* – 1)-й ошибками *j*-го вида, равное $T_i^j = i_i^j - t_{вi-1}^j$; τ_i^j – случайное время, связанное с обнаружением (поиском) *i*-й ошибки *j*-го вида, равное $\tau_i^j = t_{пi}^j - t_i^j$; θ_i^j – случайное время устранения *i*-й ошибки *j*-го вида, равное $\theta_i^j = t_{вi}^j - t_{пi}^j$; ξ_i^j – случайное время восстановления работоспособности (обнаружение ошибки и ее устранение) компонента после *i*-й ошибки *j*-го вида, равное $\xi_i^j = t_{вi}^j - t_i^j$.

Рассмотрим первую ($j = 1$) из упомянутых выше ошибок, а именно «Произошла несанкционированная очистка (обнуление) индекса СКА».

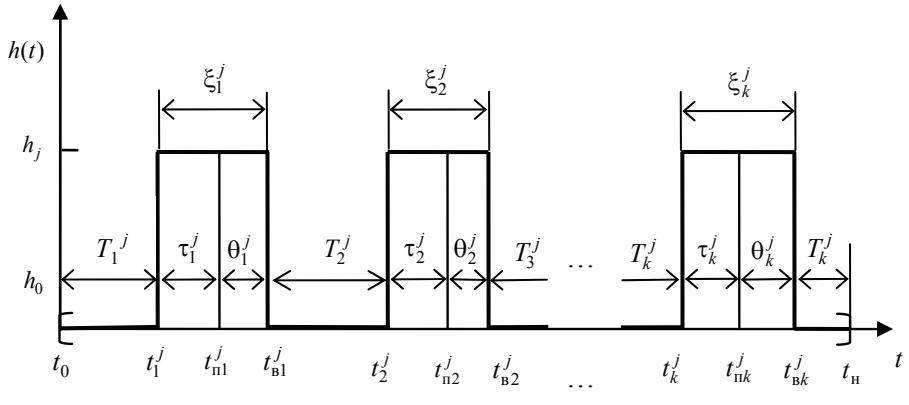

Рис. 2. Возможная траектория изменения во времени состояния функционирования $h(t)$ компонента СКА на выбранном интервале наблюдения $[t_0, t_н]$ в связи с появлением ошибки *j*-го вида

Причинами ее возникновения могут быть несанкционированные остановка службы индексирующего сервера на уровне операционной системы или перезагрузка аппаратного сервера, на котором установлено СКА как СЗИ, в момент очередного обновления индекса СКА. Ошибка не приводит к полной утрате работоспособности СКА, который продолжает функционировать, но с пониженной эффективностью.

В журнале работы индексирующего сервера запись об этой ошибке в общем виде выглядит следующим образом:

[1120] [C:\SKA\2010-12-30\Index\Index.lbx] Reset index!

Здесь ключевой является фраза «Reset index!», означающая очистку индекса. Информация в квадратных скобках характеризует место расположения файла индекса на жестком диске аппаратного сервера.

При анализе журнала работы индексирующего сервера за время наблюдения $[t_0, t_н]$ (в течение первых 9 месяцев 2011 г.) было обнаружено всего две записи о появлении данной ошибки:

21.04.2011:09:18:32.133 [1120] [C:\SKA\2011-04-08\ Index\Index.lbx] Reset index! (1)

28.06.2011:11:08:00.298 [2556] [C:\SKA\2011-06-21\ Index\Index.lbx] Reset index! (2)

Записи (1), (2) говорят о том, что в разное время произошли первая и вторая ошибки первого вида.

Восстановление индексирующего сервера в работоспособное состояние, а значит и возвращение СКА в состояние нормальной работоспособности, начиналось сразу же, то есть в момент появления этих ошибок. Оно производилось автоматически с помощью повторной индексации всех данных, поступивших в его ХД за все время функционирования СКА. Таким образом, время восстановления в этом случае было равно времени устранения ошибки и не включало времени ее обнаружения.

В журнале работы запись о завершении восстановления индекса в общем виде выглядит следующим образом:

[1304] Indexed documents: XXX, size: YYY.

Здесь фраза «Indexed documents» означает «Проиндексировано документов»; XXX – количество проиндексированных документов, YYY – суммарный размер документов.

Записи о восстановлении индекса после первой и второй ошибок имели вид:

21.04.2011:11:18:40.788 [1304] Indexed documents: 130119, size: 26543511550; (3)

28.06.2011:12:35:06.366 [1664] Indexed documents: 118747, size: 15275183954. (4)

В частности из записи (3) видно, что в момент, когда произошла первая ошибка, индекс содержал 130 119 документов и имел объем в 26 543 511 550 Б или 24,72 ГБ.

Пользуясь записями (1) – (4), вычислим значения времен T_i^1, τ_i^1, θ_i^1 и ξ_i^1 ($i = \overline{1,2}$), характеризующих процесс смены состояний функционирования $h(t)$ индексирующего сервера на выбранном интервале наблюдения для ошибки первого вида.

Время до первого появления ошибки равно $T_1^1 = t_1^1 - t_0^1$, где t_1^1 определялось из фрагмента «21.04.2011:09:18:32.133» записи (1), а $t_0^1 = 0$. Время нормальной работы компонента до второй ошибки равно $T_2^1 = t_2^1 - t_{в1}^1$, где t_2^1 определялось из фрагмента «28.06.2011:11:08:00.298» записи (2), а $t_{в1}^1$ – из фрагмента «21.04.2011:11:18:40.788» записи (3). В результате было получено, что $T_1^1 = 2649{,}3$ ч, а $T_2^1 = 1392$ ч.

Времена обнаружения ошибок $\tau_1^1 = 0$ и $\tau_2^1 = 0$, поскольку устранение ошибок начиналось сразу же после их появления. Соответственно время восстановления компонента после первой и второй ошибок в этом случае равно $\theta_1^1 = \xi_1^1$ и $\theta_2^1 = \xi_2^1$.

Естественно, что время восстановления работоспособности после первой ошибки равно $\xi_1^1 = t_{в1}^1 - t_1^1$, где $t_{в1}^1$ определялось из фрагмента «21.04.2011:11:18:40.788» записи (3), а t_1^1 – из фрагмента «21.04.2011: 09:18:32.133» записи (1). Время восстановления работоспособности индексирующего сервера после второй ошибки равно $\xi_2^1 = t_{в2}^1 - t_2^1$, где $t_{в2}^1$ определялось из фрагмента «28.06.2011:12:35:06.366» записи (4), а t_2^1 – из фрагмента «28.06.2011:11:08:00.298» записи (2). В результате было получено, что $\xi_1^1 = 2$ ч, $\xi_2^1 = 1{,}45$ ч.

Подобные вычисления проделаны на рассматриваемом интервале наблюдения $[t_0, t_н]$ для других видов ошибок ($j = 2, 3, 4$) и получены соответствующие значения времени: безотказной работы, поиска, устранения и восстановления для индексирующего сервера и модуля-посредника СКА.

Имея достаточно представительную выборку подобных результатов, получаемых с использованием предложенной в статье методики за более продолжительный период наблюдения, можно в дальнейшем определить с достаточной точностью оценки всевозможных показателей надежности индексирующего сервера, модуля-посредника и, в целом СКА, которые характеризуют их состояния с точки зрения надежности на момент вычисления этих показателей.

Естественно, что в полной мере сказанное относится ко всем средствам защиты информации, о которых было упомянуто в данной статье, а именно: АПО, СКПВВ, МСЭ, СОА и др.

Выводы

1. Систематически применяя предложенную в статье методику, можно по данным текущей эксплуатации, получаемым от средств защиты информации, расположенных на нижнем уровне системы мониторинга инцидентов информационной безопасности банка, получать постоянно обновляемые сведения, характеризующие надежность как отдельных компонентов этих средств защиты, так и каждого из них в отдельности, то есть, по сути, проводить мониторинг надежности средств защиты информации.

2. Такие сведения необходимы администратору безопасности, поскольку они позволяют ему снизить уровень неопределенности в процессе принятия решений по выявленным инцидентам информационной безопасности за счет того, что он будет получать более достоверные данные об истинном состоянии работоспособности средств защиты информации.

3. В настоящий момент применение данной методики предполагает проведение администратором безопасности весьма трудоемкого анализа журналов работы СЗИ за длительный период их функционирования. В связи с этим возникает необходимость в последующей разработке автоматизированных методов анализа журналов работы, которые бы позволили разгрузить администратора от этой дополнительной, хотя и крайне необходимой, деятельности.

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 18044–2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Введ. 2007–12–27. – М. : Стандартинформ. – 2009. – 46 с.

2. Контур информационной безопасности SearchInform [Электронный ресурс] // SearchInform. – 2010. – Режим доступа : http://www.searchin-form.ru/search-download/infosecurity_broshure_full.pdf. – Загл. с экрана.

3. Муромцев, Д.Ю. Анализ и синтез радиосистем на множестве состояний функционирования / Д.Ю. Муромцев, Ю.Л. Муромцев // Вестн. Тамб. гос. техн. ун-та. – 2008. – Т. 14, № 2. – С. 241–251.

4. Отт, А. О контентной фильтрации [Электронный ресурс] / А. Отт // JetInfo. – 2006. – Режим доступа : http://www.jetinfo.ru/2006_detail/?pid=1cbe52c11cecade331f50e34cdc2f6b5&nid=3d1031ce6c077c98fa75a7238aad4d0b&alias=2006. – Загл. с экрана.

5. Попов, С.В. Факторы, влияющие на эффективность мониторинга инцидентов информационной безопасности в автоматизированной банковской системе / С.В. Попов, В.Н. Шамкин // Науч.-техн. вестн. Поволжья. – 2010. – № 1 – С. 145–148.

6. Попов, С.В. О влиянии состояний функционирования средств защиты информации на эффективность мониторинга инцидентов информационной безопасности банка / С.В. Попов, В.Н. Шамкин // Вест. Тамб. гос. техн. ун-та. – 2011. – Т. 17, № 2. – С. 297–303.

7. Попов, С.В. Возможные состояния функционирования средств защиты информации в системе мониторинга инцидентов информационной безопасности / С.В. Попов, В.Н. Шамкин // Новые технологии и инновационные разработки : мат. 4-й межвуз. науч.-практ. конф., Тамбов, 13 мая 2011 г. / Тамб. гос. техн. ун-т. – Тамбов, 2011. – С. 69–72.

8. Попов, С.В. Мониторинг состояний функционирования средств защиты информации в информационной системе / С.В. Попов, В.Н. Шамкин // Тр. междунар. науч.-техн. конф. «Современные информационные технологии» "Contemporary Information Technologies" (Computer-Based Conference) / Пенз. гос. технол. акад. – Пенза, 2011. – Вып. 13. – С. 165–168.

9. Buttcher, S. Information Retrieval. Implementing and Evaluating Search Engines / S. Buttcher, C. Clarke, G. Cormack. – Cambridge : The MIT Press, 2010. – 631 p.

10. The Top Ten Insider Threats and How to Prevent Them [Электронный ресурс] // Prism Microsystems. – 2010. – Режим доступа : http://www.bank-infosecurity.com/whitepapers.php?wp_id=432. – Загл. с экрана.

Method of Monitoring Reliability Parameters of Information Security Devices in Bank Using their Current Operating Data

S.V. Popov, V.N. Shamkin

Tambov State Technical University, Tambov

Key words and phrases: content analysis; information security; information security event; information security incident; log; malfunctioning; reliability parameters.

Abstract: The paper presents the method enabling the administrator to receive regularly updated data from data protection logs located on the lower level of the bank security system. These data characterizes reliability of separate components of these means of protection, as well as each of them separately.
