УДК 681.518.5

О ВЛИЯНИИ СОСТОЯНИЙ ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ЭФФЕКТИВНОСТЬ МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

С.В. Попов, В.Н. Шамкин

Кафедра «Конструирование радиоэлектронных и микропроцессорных систем», ГОУ ВПО «ТГТУ»; posevik@yandex.ru

Представлена членом редколлегии профессором В.И. Коноваловым

Ключевые слова и фразы: защита информации; инцидент информационной безопасности; мониторинг; событие информационной безопасности; состояние функционирования; эффективность.

Аннотация: На основе проведенного анализа влияния различных факторов на эффективность мониторинга инцидентов информационной безопасности в автоматизированной банковской системе обоснована необходимость разработки подсистемы, позволяющей повысить уровень защищенности конфиденциальной информации.

Аббревиатуры

АБС – автоматизированная банковская система;	МИИБ – мониторинг инцидентов ИБ;
АС – автоматизированная система;	ПОИБ – подсистема обеспечения ИБ;
ИБ – информационная безопасность;	СЗИ – средство защиты информации;
ИИБ – инцидент информационной безопасности;	СИБ – система ИБ;
	СМИИБ – система МИИБ;
КИ – конфиденциальная информация;	СоИБ – событие ИБ

Введение

Система информационной безопасности банка представляет собой совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение [1]. Система обеспечения информационной безопасности банка – это совокупность СИБ и системы менеджмента информационной безопасности [2]. При этом группы процессов системы менеджмента организуют в виде циклической модели Деминга «… – планирование – реализация – проверка – совершенствование – планирование – …», являющейся основой модели менеджмента в стандартах качества [3, 4].

С помощью мониторинга ИБ, который является одним из элементов системы менеджмента банка, ведется как оперативное, так и постоянное наблюдение, осуществляется сбор, анализ и обработка данных под заданные руководством цели, связанные с защитой банковской информации.

Значение мониторинга информационной безопасности для обеспечения защиты банковской информации

По мнению Б. Шнаера, «Мониторинг – это окно компании в ее собственную безопасность» [5].

Выделим следующие аспекты, связанные с обеспечением ИБ банка, которые в значительной степени определяют значимость своевременного и эффективного мониторинга.

Во-первых, выявление в реальном времени нарушений ИБ и адекватное реагирование на них. Связано это с тем, что администраторы безопасности не всегда могут уделить своевременное и должное внимание процессам получения и последующего анализа данных, поступающих от многочисленных средств защиты информации (антивирусы, межсетевые экраны, системы обнаружения вторжений и т.д.).

Во-вторых, обеспечение непрерывности мониторинга событий, связанных с деятельностью персонала (вход в систему, использование портов ввода/вывода, запись информации на внешние носители и др.) и внешних нарушителей (попытки несанкционированного доступа в сеть банка, проведение вирусных атак, провоцирование отказов в обслуживании и др.) [6]. Постоянное и непрерывное наблюдение за происходящим в АБС позволяет обеспечить ее защищенность.

В-третьих, возможность обнаружения применения злоумышленниками новых средств и методов несанкционированного и противоправного получения КИ, появившихся в результате развития новых информационных технологий. Реализация этой возможности требует наличия определенного интеллекта в СИБ.

Несвоевременность определения нарушений ИБ и непринятие адекватных мер по защите КИ могут привести к существенному снижению уровня защищенности, обеспечиваемого СИБ. Поэтому, необходима разработка такой процедуры мониторинга и последующего ее осуществления, которые позволили бы СИБ своевременно выявлять различные, в том числе и ранее неизвестные, угрозы ИБ.

В отсутствие такой процедуры, банк будет на несколько шагов отставать от действий внешних или внутренних злоумышленников, а также узнавать о произошедших утечках информации из внешних источников, что не может не повлечь за собой крупных финансовых и репутационных потерь.

Далее рассматриваются вопросы, связанные с МИИБ, который является важным этапом обеспечения ИБ АБС [7].

Факторы, влияющие на эффективность мониторинга инцидентов информационной безопасности

Согласно [8], АБС включает в себя три АС: «Управление банком»; «Операционный день банка»; «Банковские электронные услуги», каждая из которых выполняет определенные функции и имеет свою ПОИБ. Предлагается информацию обо всех событиях ИБ направлять из ПОИБ каждой АС на последующий анализ в СМИИБ (рис. 1) с целью выявления всех инцидентов ИБ, происходящих в АБС и принятия соответствующих мер.

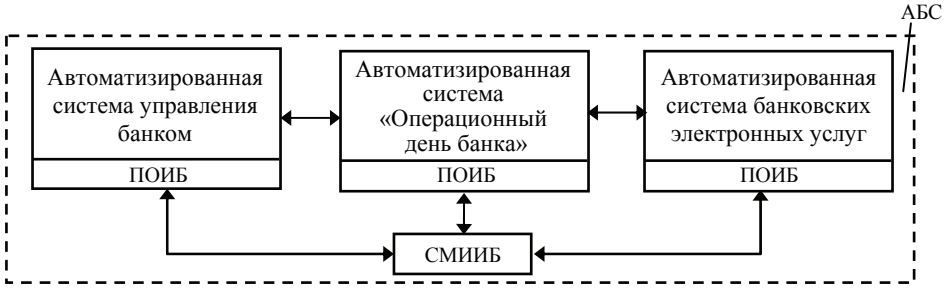

Рис. 1. Место СМИИБ в структуре АБС

Под СоИБ будем понимать идентифицированное появление определенного состояния системы, сервиса или сети, которое свидетельствует либо о возможном нарушении политики информационной безопасности банка или отказе защитных мер, либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности. Соответственно ИИБ – это появление одного или нескольких нежелательных или неожиданных СоИБ, с которыми связана значительная вероятность создания угрозы ИБ [9].

Структурная схема СМИИБ представлена на рис. 2.

Основными компонентами системы являются:

− центральная консоль мониторинга (**ЦКМ**), предназначенная для управления и настройки системы, отображения информации о состоянии ИБ в АБС, вывода извещений об инцидентах и выдачи рекомендаций по их устранению;

− база данных инцидентов (**БДИ**), используемая для хранения выявленных инцидентов;

− база данных событий (**БДС**), служащая для хранения всех поступивших от СЗИ событий ИБ, в том числе не являющихся инцидентами;

− база знаний экспертов (**БЗЭ**), содержащая экспертные знания, используемые МВИ при выявлении инцидентов ИБ;

− модуль выявления инцидентов (**МВИ**) – автоматизированное ядро системы, анализирующее данные, которые поступают от СЗИ, и предлагающее администратору безопасности меры по устранению обнаруженных угроз ИБ, а в отдельных случаях и устраняющее их;

− модуль управления архивными журналами (**МУАЖ**), отвечающий за запись событий в БДС, а также за их извлечение по запросу с ЦКМ;

− сборщики событий ($СС_i$, $i = 1, 2, ..., n$), которые используются для нормализации данных, полученных от СЗИ, то есть приведения их к единому формату, используемому МВИ.

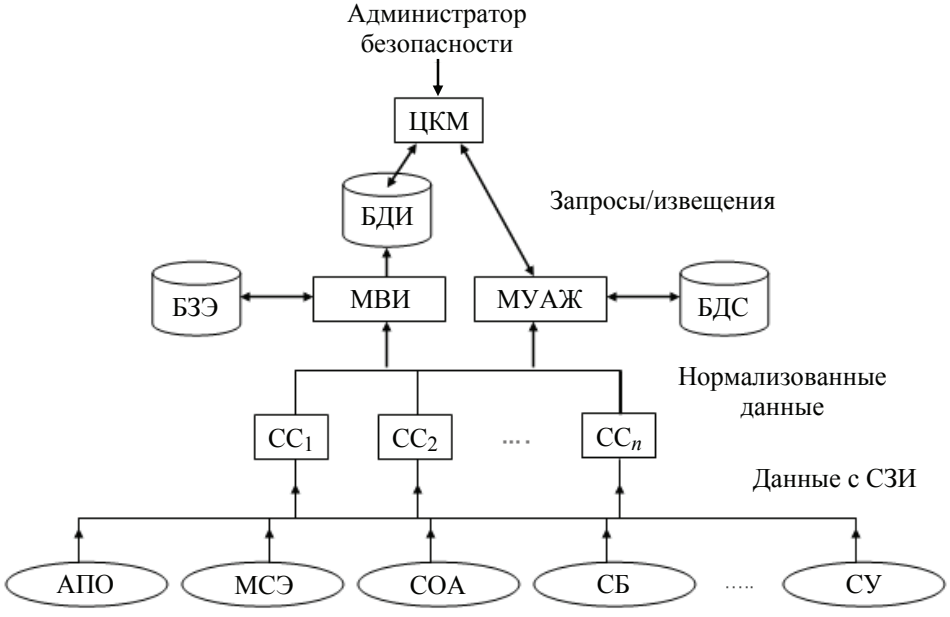

Рис. 2. Структурная схема СМИИБ

На нижнем уровне системы располагаются различные программно-аппаратные СЗИ, собирающие данные о СоИБ:

− антивирусное ПО (**АПО**);
− межсетевые экраны (**МСЭ**);
− системы обнаружения атак (**СОА**);
− серверы безопасности (**СБ**);
…
− сетевые устройства (**СУ** – маршрутизаторы, концентраторы и т.д.).

Администратор безопасности СМИИБ принимает окончательное решение по устранению выявленных ИИБ и следит за их своевременной реализацией.

Заметим, что в силу действия различных факторов, реальный результат мониторинга может отличаться от желаемого – обнаружения всех ИИБ. Естественно, что чем меньше различие между реальным и желаемым результатами, тем мониторинг эффективнее. Для повышения эффективности процесса МИИБ необходимо вначале выявить факторы, негативно влияющие на мониторинг, а затем, по возможности, устранить их влияние.

Система МИИБ при оперативном выявлении инцидентов за приемлемое время должна обрабатывать значительный объем данных о СоИБ, получаемых от СЗИ, при этом на процесс выявления среди СоИБ инцидентов оказывают влияние параметры как программного, так и аппаратного обеспечения различных компонентов системы.

В наибольшей степени на результат мониторинга влияют следующие факторы:

1) своевременность обнаружения инцидента;

2) наличие и возможность пополнения знаний о вероятных инцидентах.

Рассмотрим первый из этих факторов. Именно от него зависит материальный или репутационный ущерб для банка, связанный с запаздыванием в адекватном реагировании на соответствующий инцидент. Например, запаздывание в реагировании на ИИБ в 10 ч приводит к 80 % успеха злоумышленника, при 20 ч – к 95 % его успеха, а при 30 ч – успех злоумышленника гарантирован в любом случае [10].

Следует выделять время поступления данных с СЗИ на обработку в МВИ и, собственно, время их обработки этим модулем.

Время поступления данных в МВИ зависит, главным образом, от характеристик конкретных СЗИ и каналов передачи данных между компонентами СМИИБ:

− работоспособности СЗИ (сбои могут быть вызваны как физическими или программными отказами устройств, так и преднамеренными действиями злоумышленников) [11–13];

− настройки СЗИ (плохо настроенное СЗИ способно обнаруживать ложные СоИБ, которые, при большом их числе, могут спровоцировать персонал к игнорированию действительных СоИБ, полученных от данного СЗИ) [11];

− пропускной способности каналов передачи данных (в качестве последних используются те же телекоммуникационные каналы, что и в АБС, из-за чего на них создается повышенная нагрузка).

Время обработки данных, поступивших в МВИ с СЗИ, зависит:

− от работоспособности МВИ (физический или программный отказ МВИ способен нарушить процесс мониторинга, вплоть до полного прекращения обработки поступающей информации о СоИБ);

− наличия очереди из сообщений о СоИБ (вновь пришедшие на обработку сообщения могут оказаться сообщениями об ИИБ и могут быть выявлены слишком поздно для предотвращения возможного ущерба).

Рассмотрим второй из упомянутых ранее факторов, в наибольшей степени влияющий на результат мониторинга инцидентов. Имеется в виду наличие и возможность пополнения знаний, необходимых для выявления ИИБ из множества сообщений о СоИБ, поступивших в МВИ на обработку. При этом следует говорить о сигнатурах и накопленном персоналом опыте по выявлению ИИБ.

Сигнатуры – отличительные признаки и характеристики конкретных ИИБ могут варьироваться от весьма простых (строка символов, отвечающая одной определенной команде) до сложных (изменение состояния безопасности, сформулированное в виде формального математического выражения) [14].

Очевидно, что результаты мониторинга зависят:

− от существования сигнатур для конкретных ИИБ (создание сигнатур для ранее неизвестных ИИБ занимает некоторое время, в течение которого выявить соответствующий инцидент ИБ невозможно);

− целостности сигнатур (в случае изменения злоумышленником или вредоносным процессом содержимого сигнатур, хранящихся на жестких дисках или в оперативной памяти использующих их СЗИ, СМИИБ не сможет выявить соответствующие ИИБ);

− возможности обновления сигнатур (к нарушениям процесса обновления приводят ошибки в настройке СЗИ, сбои программно-аппаратных компонентов СМИИБ и т.д.).

Накапливаемый персоналом опыт, связанный с идентификацией новых, неизвестных ранее, инцидентов, для которых сигнатурное выявление было невозможно, целесообразно представлять в виде экспертных знаний, которые могут быть использованы в СМИИБ при наличии в ней подсистем получения и накопления знаний.

Необходимость разработки подсистемы определения состояний функционирования системы мониторинга инцидентов информационной безопасности

В процессе эксплуатации АБС администратору безопасности приходится оценивать влияние, оказываемое перечисленными факторами на эффективность работы СМИИБ, а, следовательно, и на обеспечение общей защищенности КИ в АБС. Заметив отклонение текущего состояния СМИИБ от нормального состояния, характеризуемого конкретными значениями ряда показателей, администратор стремится найти причину этого отклонения, то есть выявить фактор, оказавший влияние на процесс мониторинга. Чтобы квалифицированно сделать это он должен затратить определенное время и обладать необходимыми компетенциями, которые, как правило, формируются в результате длительного опыта. Если выявленный фактор оказывает негативное влияние (например, из-за сбоя в межсетевом экране не будут поступать в СМИИБ сообщения о сканировании портов), то администратор совершает корректирующие действия, приводящие к восстановлению нормального состояния СМИИБ (например, перенастраивает межсетевой экран). Если выявлены причины позитивного изменения состояния СМИИБ, то последнее принимается за нормальное состояние и, соответственно, корректируются значения показателей, характеризующих это состояние.

Поскольку парк СЗИ в АБС постоянно пополняется новыми средствами защиты и значительно возрастает нагрузка на администраторов безопасности, то представляется целесообразным автоматизировано собирать данные, характеризующие состояние СМИИБ, определяя состояния функционирования СЗИ, обрабатывать эти данные и периодически выдавать информацию администратору безопасности для принятия им последующих решений.

Заключение

Предлагается в системе мониторинга инцидентов информационной безопасности создать подсистему определения ее состояний функционирования, которая позволит повысить эффективность обнаружения инцидентов и соответствующего реагирования на них, а, следовательно, обеспечить более высокий уровень защищенности конфиденциальной информации в автоматизированной банковской системе.

Список литературы

1. Стандарт Банка России СТО БР ИББС-1.0-2008 // Вестн. Банка России. – 2009. – № 2 (1093) – 38 с.
2. Курило, А.П. О новой редакции Стандарта Банка России «Обеспечение информационной безопасности организации банковской системы Российской Федерации. Общие положения» / А.П. Курило // Деньги и кредит. – 2009. – № 2 (1093). – С. 3–7.
3. ГОСТ Р ИСО 9001–2008. Системы менеджмента качества. Требования. – Взамен ГОСТ Р ИСО 9001–2001 ; введ. 2009–11–13. – М. : Стандартинформ, 2008. – 65 с.
4. ISO/IEC IS 27001–2005. Information Technology. Security Techniques. Information Security Management Systems. Requirements. – Switzerland : ISO/IEC, 2005. – 34 с.
5. Schneier, B. Managed Security Monitoring: Network Security for 21th Century / B. Schneier. – Counterpane Internet Security, Inc., 2005. – 6 p.
6. Инсайдерские угрозы в России ’09 [Электронный ресурс] / Perimetrix. – 2009. – Режим доступа : http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pdf. – Загл. с экрана.
7. Попов, С.В. Значение мониторинга информационной безопасности для обеспечения защиты банковской информации / С.В. Попов, В.Н. Шамкин // Прогрессивные технологии развития : сб. материалов 6-й междунар. науч.-практ. конф., Тамбов, 27–28 дек. 2009 г. / Тамб. гос. техн. ун-т. – Тамбов, 2009. – С. 54–56.
8. Додонова, И.В. Автоматизированная обработка банковской информации: учеб. пособие / И.В. Додонова, О.В. Кабанова. – М. : КНОРУС, 2008. – 176 с.
9. 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.
10. Семенов, Ю.А. Сетевая безопасность, состояние и перспективы / Ю.А. Семенов // Информ. технологии и вычисл. техника. – 2007. – № 4. – С. 70–87.
11. Fry, Ch. Security Monitoring / Ch. Fry, M. Nystrom. – Sebastopol : O’Reilly, 2009. – 227 p.
12. Сердюк, В.А. Новое в защите от взлома корпоративных систем / В.А. Сердюк. – М. : Техносфера, 2007. – 360 с.
13. Перегуда, А.И. Математическая модель надежности систем защиты информации / А.И. Перегуда, Д.А. Тимашов // Информ. технологии. – 2009. – № 8. – С. 10–17.
14. Кочнев, В.Ф. Обнаружение нелегального пользователя компьютерной системы : учеб. пособие / В.Ф. Кочнев, Е.В. Титов, С.А. Филиппов. – М. : МИИТ, 2003. – 48 с.

On the Influence of Functioning State of Data Protection Tools on the Efficiency of Monitoring of Bank Information Security Incidents

S.V. Popov, V.N. Shamkin

Department "Designing of Radioelectronic and Microprocessor Systems", TSTU; posevik@yandex.ru

Key words and phrases: efficiency; functioning state; information security; information security event; information security incident; monitoring.

Abstract: On the basis of the analysis of influence of various factors on the efficiency of monitoring of information security incidents in the automated bank system the paper justifies the necessity of the subsystem development, enabling to raise the level of security of the confidential information.

Über Einwirckung der Zustände des Funktionierens der Mittel des Informationsschutzes auf die Effektivität des Monitorings der Zwischenfälle der Informationssicherheit der Bank

Zusammenfassung: Auf Grund der durchgeführten Analyse der Einwirckung der verschiedenen Faktoren auf die Effektivität des Monitorings der Zwischenfälle der Informationssicherheit im automatisierten Bankensystem wird die Notwendigkeit der Erarbeitung des Subsystems, das das Niveau der Sicherheit der vertraulichen Information zu erhöhen erlaubt, begründet.

Sur l'influence de l'état du fonctionnement des moyens de la protection de l'information sur l'efficacité du monitoring des incidents de la sécurité informatique de la banque

Résumé: À la base de la réalisation de l'analyse de l'influence de différents facteurs sur l'efficacité du monitoring des incidents de la sécurité informatique dans un système bancaire autonome est argumentée la nécessité de l'élaboration du sous-système permettant d'augmenter le niveau de la protection de son information confidentielle.

Авторы: ***Попов Сергей Викторович*** – аспирант кафедры «Конструирование радиоэлектронных и микропроцессорных систем»; ***Шамкин Валерий Николаевич*** – доктор технических наук, профессор кафедры «Конструирование радиоэлектронных и микропроцессорных систем», ГОУ ВПО «ТГТУ».

Рецензент: ***Муромцев Дмитрий Юрьевич*** – доктор технических наук, заведующий кафедрой «Конструирование радиоэлектронных и микропроцессорных систем», ГОУ ВПО «ТГТУ».