УДК 681.518.3
DOI: 10.17277/vestnik.2020.02.pp.176-187

УСОВЕРШЕНСТВОВАНИЕ ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ РАБОТОСПОСОБНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

Д. Ю. Муромцев[1], С. В. Попов[2], В. Н. Шамкин[1]

Кафедра «Конструирование радиоэлектронных и микропроцессорных систем» (1), crems@mail.jesby.tstu.ru; ФГБОУ ВО «ТГТУ», г. Тамбов, Россия; кафедра безопасности и информационных технологий (2), popovsvik@mpei.ru; ФГБОУ ВО «Национальный исследовательский университет «МЭИ», г. Москва, Россия

Ключевые слова: блок оценки надежности; вероятности состояний функционирования; информационная безопасность; оценка работы; подсистема обеспечения работоспособности; средства защиты информации.

Аннотация: Дано описание подсистемы обеспечения работоспособности в системе мониторинга инцидентов информационной безопасности, в которую введен разработанный авторами блок оценки надежности средств защиты информации по данным текущей эксплуатации. Проведена оценка работы системы мониторинга до и после начала использования усовершенствованной подсистемы обеспечения работоспособности.

Аббревиатуры

АБ – администратор безопасности;
АБС – автоматизированная банковская система;
БД – база данных;
БОНСЗИ – блок оценки надежности средств защиты информации;
БР – блок резервирования;
БХДР – блок хранения данных резервирования;
ИБ – информационная безопасность;
ИИБ – инцидент информационной безопасности;
ПАС – программно-аппаратное средство;
ПД – персональные данные;
ПОРС – подсистема обеспечения работоспособности СМИИБ;
СЗИ – средство защиты информации;
СКА – средство контентного анализа;
СМИИБ – система мониторинга инцидентов информационной безопасности

Введение

В статье предлагается реализовать в системе мониторинга инцидентов информационной безопасности, входящей в АБС, приведенные ранее в [1 – 7] методики и алгоритмы.

Разрабатывается ПОРС, которая объединит уже существующие средства обеспечения работоспособности отдельных СЗИ и где будет использована идеология аналогов подобных подсистем в информационных системах других предметных областей. В создаваемую подсистему предлагается ввести отдельный блок, с помощью которого будут оперативно оцениваться вероятности состояний функционирования СЗИ по данным, регулярно обновляемым в процессе текущей эксплуатации СМИИБ.

Для оценки работы усовершенствованной СМИИБ необходимо вычислить и сравнить показатели, характеризующие выявление инцидентов информационной безопасности в АБС за некоторый промежуток времени до и после внедрения ПОРС.

Подсистема обеспечения работоспособности системы мониторинга

Одной из важнейших задач в СМИИБ является поддержание работоспособности СЗИ, входящих в ее состав. В банках для осуществления контроля нормального функционирования отдельных компонентов СМИИБ используются технические средства, а часть функций по контролю возлагается на администратора безопасности. Успешное выполнение данной задачи осложняется наличием большого количества СЗИ разных типов и недостаточностью объема нужной информации об их текущем функционировании, что затрудняет АБ своевременное получение необходимой информации в нужном объеме, а также ее последующий анализ и принятие, при необходимости, соответствующих мер по восстановлению работоспособности СЗИ.

В современных информационных системах используются автоматизированные средства, совокупность которых оформляется в виде отдельных подсистем обеспечения работоспособности, осуществляющих контроль нормального функционирования различных ПАС. К основным методам их работы относятся [8 – 16]:

– резервирование файлов конфигураций ПАС, позволяющее восстановить параметры функционирования в случае несанкционированного их изменения;

– мониторинг системных показателей ПАС: уровня использования ресурса центрального процессора; объемов используемой оперативной памяти, файлов подкачки, свободного дискового пространства; производительности локальной сети и др.;

– создание «снимков» параметров оптимально функционирующих ПАС и сравнение с ними реальных параметров;

– отслеживание критически важных процессов и служб, необходимых для функционирования ПАС;

– применение программного обеспечения, предназначенного для автоматического устранения нарушений работоспособности ПАС;

– анализ журналов работы компонентов ПАС на наличие записей об ошибках;

– применение средств активного обнаружения ошибок в программных средствах;

– мониторинг сетевой доступности ПАС.

В качестве примера можно назвать следующие системы: Zenoss, Nagios и Zabbix [14, 17, 18].

Применительно к работе СМИИБ банков следует предложить дополнительно использовать следующие методы осуществления контроля работоспособности [8, 9, 11, 19]:

– проверка целостности информационных и функциональных ресурсов СЗИ, входящих в СМИИБ;

– генерация событий-маркеров;

– различные проверки модулей хранения информации (базы знаний экспертов, данных событий и инцидентов ИБ).

На основе применения вышеперечисленных методов разрабатывается подсистема обеспечения работоспособности СМИИБ, в которой также используются результаты, полученные авторами в [1 – 7].

На рисунке 1 представлена структурная схема ПОРС, в которую входят следующие компоненты:

– *консоль*, позволяющая осуществлять наблюдение за процессом работы ПОРС и управление им, которая может работать как вместе с центральной консолью мониторинга СМИИБ (см. рис. в [1]), так и независимо, в случае ее недоступности (по различным причинам).

– *блок оценки надежности средств защиты информации*, выделенный серым цветом и являющийся принципиально новым блоком.

– *блок резервирования*, осуществляющий сбор и сохранение файлов настроек (параметров работы) СЗИ, а также создающий образы оптимально функционирующих средств.

– *блок хранения данных резервирования*, представляющий собой хранилище, в котором содержатся собранные БР данные.

– *блок контроля целостности*, контролирующий целостность файлов, ветвей реестра на удаленных узлах (рабочих станциях, серверах или СЗИ), содержимого оперативной памяти и БД [8].

– *генератор событий-маркеров*, совершающий с заданной периодичностью определенные действия, называемые событиями-маркерами [9], которые имитируют вредоносную деятельность, направленную на информационные ресурсы АБС.

– *блок автоматической обработки событий*, предназначенный для устранения в автоматическом режиме некоторых нарушений, возникающих в СМИИБ.

– *агенты*, осуществляющие сбор необходимых для работы ПОРС данных со всех подключенных СЗИ.

Рассмотрим работу некоторых из вышеперечисленных компонентов.

В блоке резервирования осуществляется резервирование двух типов.

Резервирование конфигураций направлено на поддержание файлов настроек СЗИ в состоянии, определенном администратором. Оно проводится перед каждым внесением изменений в файлы настроек. Копии файлов отдельно взятого СЗИ

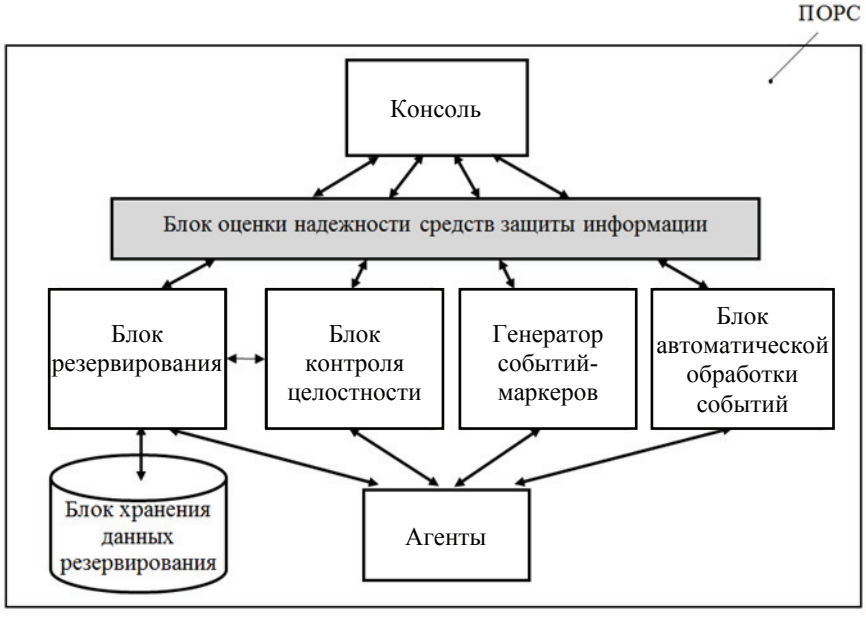

Рис. 1. Структурная схема подсистемы обеспечения работоспособности СМИИБ

сохраняются в БХДР, причем последняя копия считается эталонной. Периодически файлы текущих настроек СЗИ сравниваются с эталонными на предмет наличия в них несанкционированных, то есть неподтвержденных администратором, изменений. Если такие изменения обнаруживаются, то файл текущих настроек автоматически заменяется эталонным. Во избежание замены эталонным файлом нового файла, санкционированного администратором, вводится процедура подписи файла настроек секретным ключом администратора.

Резервирование оптимально функционирующего средства заключается в создания образа (в полном копировании) внутренней памяти СЗИ или жесткого диска физического сервера, на котором данное СЗИ развернуто, а полученные образы сохраняются в БХДР. При этом во время такого резервирования по локальной сети банка передается значительный объем данных, что может нарушить работу как самой СМИИБ, так и частично АБС. По этой причине все операции по созданию образов оптимально функционирующих средств проводятся в нерабочие часы.

В блоке хранения данных резервирования сохраняются полученные от БР данные двумя различными способами: в виде записей в БД и в виде файлов на жестких дисках физических серверов, взаимодействующих со СМИИБ.

Блок контроля целостности сравнивает наборы текущих значений параметров конкретных СЗИ, которые могут (в зависимости от типа и модели СЗИ) содержаться в файлах, реестре, БД и т.д., с эталонными наборами значений параметров для этих СЗИ. Если наборы не отличаются, то это говорит о целостности параметров СЗИ, в противном случае – о произошедшем нарушении.

Генератор событий-маркеров проверяет, путем моделирования возможных атак на АБС, исправность СЗИ и их готовность обнаруживать и отражать данные атаки. Для различных СЗИ, входящих в состав СМИИБ, используются разные события-маркеры. Например, для межсетевого экрана или средства обнаружения атак таким событием может являться сканирование с заданной периодичностью определенного сервера или рабочей станции в АБС, а для антивирусного программного обеспечения – имитация на сервере или рабочей станции действий, характерных для функционирования вредоносных программ.

Блок автоматической обработки событий содержит в себе библиотеку вполне определенных наборов команд (скриптов), которые выполняются в случае возникновения различных нарушений в работе отдельных компонентов СМИИБ. Например, блок используется для удаленной перезагрузки/выключения сервиса или рабочей станции, автоматического запуска программного обеспечения, очистки места на жестком диске и т.д.

Блок оценки надежности средств защиты информации в системе мониторинга

С помощью блока оценки надежности средств защиты информации в системе мониторинга в ПОРС вычисляются значения вероятностей состояний функционирования СЗИ с использованием регулярно обновляемой (по данным текущей эксплуатации) информации о произошедших ранее нарушениях их работоспособности.

Схема информационного взаимодействия БОНСЗИ с ПОРС и СМИИБ приведена на рис. 2, из которого также видна структура рассматриваемого блока.

Вычисление значений интересующих АБ стационарных и нестационарных вероятностей состояний функционирования осуществляется в модуле определения показателей надежности СЗИ, выделенном на рис. 2 серым цветом. Данный модуль является ключевым в составе БОНСЗИ, в его основе лежит разработанная авторами процедурная модель определения вероятностей состояний функционирования СЗИ.

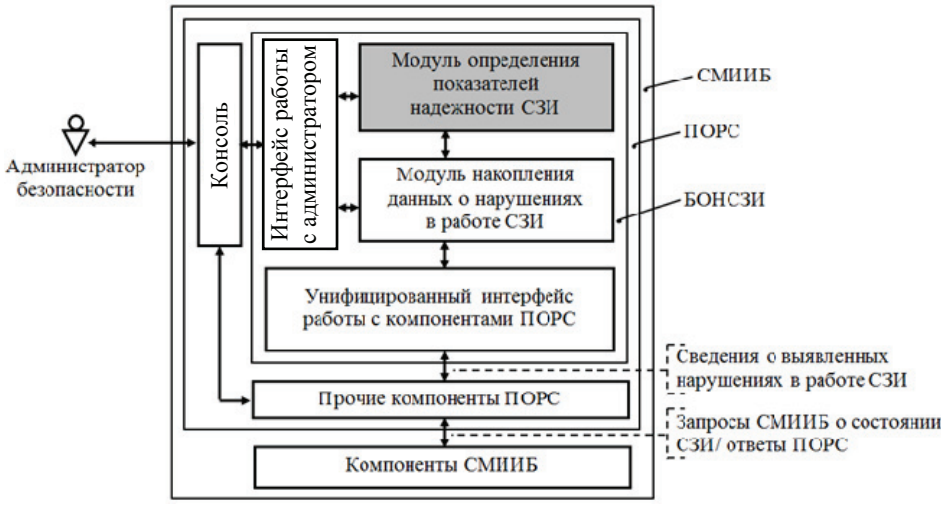

Рис. 2. Схема информационного взаимодействия БОНСЗИ с ПОРС и СМИИБ

Унифицированный интерфейс работы с компонентами ПОРС предназначен для сопряжения БОНСЗИ с разнообразными ПОРС. Интерфейс работы с АБ предназначен для передачи команд управления, поступающих в БОНСЗИ от администратора; при ручном вводе данных о произошедших нарушениях в работе СЗИ (в случае, если нарушения не были зафиксированы ПОРС, но были обнаружены АБ); для корректировки уже сохраненных данных; для передачи администратору информации о состоянии надежности СЗИ.

В модуле накопления данных о нарушениях в работе СЗИ сохраняются сведения о произошедших ранее нарушениях работы СЗИ, входящих в состав СМИИБ, которые поступают в БОНСЗИ от прочих компонентов ПОРС, представленных ранее на рис. 1, или вводятся вручную АБ.

Блок оценки надежности средств защиты информации автоматически анализирует журналы работы различных СЗИ, используя разработанную в [7] методику анализа, на предмет выявления имевших место нарушений функционирования дискретных и непрерывных СЗИ[1]. Это позволяет за меньшее (по сравнению с ручным анализом администратора) время проводить исчерпывающее исследование журналов, получать достоверную информацию о текущем функционировании СЗИ и обрабатывать ее. В результате, по информации, извлекаемой из электронных журналов, можно оперативно определять различные характеристики надежности компонентов СЗИ, которые впоследствии необходимы при оценке надежности и эффективности функционирования данных СЗИ. 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.

Проведению первого подобного анализа предшествует, как правило, начальное обучение БОНСЗИ, состоящее в том, что АБ вносит в модуль определения показателей надежности СЗИ (см. рис. 2) следующую информацию: слова, слово-

[1]СЗИ, с учетом фактора надежности, можно разделить на два вида: с непрерывным и дискретным временем работы. Данное обстоятельство определяет выбор математических методов, пригодных для исследования конкретных СЗИ с учетом нахождения в различных состояниях функционирования.

сочетания, последовательности записей и т.д., встречаемые в журналах различных СЗИ и соответствующие возникновению всевозможных нарушений в работе. В отдельных случаях БОНСЗИ изначально может содержать некоторый объем информации, необходимой для проведения анализа журналов работы.

Пересчет значений показателей надежности конкретного СЗИ осуществляется БОНСЗИ как в случае возникновения очередного нарушения в его работе, так и по расписанию при обновлении информации для всех СЗИ.

Чтобы БОНСЗИ начал в полном объеме выполнять свои функции следует затратить некоторое время для накопления в достаточном объеме необходимой информации о произошедших нарушениях в работе применяемых СЗИ (например, 2–3 года). В течение этого срока в состав СМИИБ нежелательно вносить значительные изменения.

Благодаря наличию БОНСЗИ в ПОРС, администратор безопасности может оперативно получать информацию о текущей надежности СЗИ и прогнозировать ее на будущее, поэтому он более обоснованно, чем ранее, может принимать решения по обеспечению нормальной работы СМИИБ.

Оценка работы системы мониторинга до и после применения усовершенствованной подсистемы обеспечения работоспособности

Рассуждения построены на примере одного из СЗИ дискретного типа, а именно средства контентного анализа, входящего в состав СМИИБ, которое представляет собой программно-аппаратный комплекс, предназначенный для мониторинга сетевого трафика в целях выявления нарушений политики безопасности[2] [5]. Предполагается, что ПОРС отслеживает работоспособность только СКА, подверженного нарушениям в работе, а остальные СЗИ работают без нарушений. Сделать это возможно, поскольку СЗИ функционируют независимо друг от друга.

Сравнивалось количество ИИБ, выявленных СКА, на примере системы аудита файлов, копируемых на съемные носители, в течение года, предшествующего началу использования ПОРС, и последующего. До начала использования СКА в сутки в среднем выявляло 5 923 потенциальных события ИБ[3], из которых 118 являлось инцидентами ИБ[4]. Другими словами, в среднем, примерно каждое пятидесятое событие, связанное с копированием информации на съемные носители, было потенциально опасным для банка, поскольку информация содержала конфиденциальные сведения. Соответственно, общее число ИИБ, выявленных СКА за 12 месяцев, составило 43 070.

Восстановление работы СКА после возникновения нарушения связано с его поиском и принятием мер по устранению.

Время, суммарно затраченное на восстановление работоспособности СКА по результатам расчета после обнаружения в журналах работы СКА ошибок нескольких видов, составило 4,19 суток.

Таким образом, СКА из 365 суток фактически функционировало 360,81 суток. Если разделить общее число выявленных за 12 месяцев ИИБ на это время,

[2]Выделяют несколько видов СКА [13]: различные системы аудита (почтовых сообщений; мгновенных сообщений; IP-телефонии; файлов, копируемых на съемные носители) и системы мониторинга Интернет-трафика.

[3]Событие информационной безопасности – это идентифицированное появление определенного состояния системы, сервиса или сети, которое свидетельствует либо о возможном нарушении политики ИБ банка или отказе защитных мер, либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности.

[4]Инцидент информационной безопасности – это появление одного или нескольких нежелательных или неожиданных СИБ, с которыми связана значительная вероятность создания угрозы ИБ.

то получим среднесуточное число выявляемых ИИБ при отсутствии нарушений в работе компонентов СКА

$$43070 / 360{,}81 = 119{,}37.$$

Соответственно, если бы СКА в течение года работало безошибочно, то оно должно было выявить следующее число ИИБ

$$365 \cdot 119{,}37 \approx 43570.$$

Поскольку использование ПОРС значительно сокращает (практически исключает) время, связанное с поиском ошибок в работе СКА, то, естественно, сокращается и суммарное время, затрачиваемое на восстановление работоспособности СКА. Практически сразу ПОРС известит администратора о возникшем нарушении, который сразу может начать процесс устранения.

Как показали расчеты при использовании ПОРС в течение года суммарное время восстановления работоспособности СКА составит 5,124 ч или 0,21 суток.

За это время число ИИБ, пропущенных или обнаруженных со значительным опозданием из-за нарушений в работе СКА, равно

$$0{,}21 \cdot 119{,}37 = 25{,}07 \approx 25.$$

При этом необходимо отметить, что не только пропуск ИИБ, но и его выявление с задержкой, негативно влияют на состояние ИБ в банке. Если вследствие нарушения работы СКА, инцидент не был обнаружен при ближайшей проверке по расписанию, то автоматически он может быть обнаружен не ранее, чем через несколько часов при одной из следующих проверок[5]. При этом устранение негативных последствий, связанных с ним, может оказаться крайне затруднительным.

Всего за время наблюдения после внедрения ПОРС было бы выявлено следующее число инцидентов

$$43570 - 25 = 43545.$$

Таким образом, при использовании ПОРС увеличивается «производительность» СМИИБ. За 12 месяцев наблюдения данный факт можно охарактеризовать следующим числом

$$(43545 - 43070) / 43070 = 0{,}011 \text{ или } 1{,}1\ \%.$$

Проведя подобную оценку для каждого СЗИ, входящего в СМИИБ, можно получить некоторое суммарное значение, характеризующее рост производительности СМИИБ.

Целесообразность внедрения ПОРС в СМИИБ можно оценить и по общей стоимости для банка выявленных с задержкой или не выявленных совсем ИИБ. Проиллюстрируем это также на примере СКА.

Стоимость одного ИИБ, выявляемого с помощью СКА, будем определять стоимостью для банка той информации, копирование которой вызвало возникновение этого ИИБ.

Предположим, что такой информацией являются персональные данные клиентов банка и его сотрудников. Тогда рассчитать стоимость одного ИИБ можно как произведение количества скопированных на съемный носитель записей ПД (то есть сведений об одном сотруднике или клиенте) на среднюю стоимость для банка одной такой записи.

[5]Особенностью некоторых СКА (в том числе, рассмотренного в работе) является то, что они выполняют свои функции периодически в соответствии с заданным администратором безопасности расписанием. Такой режим работы обусловлен необходимостью предварительного построения индекса или, иными словами, структуры данных, предназначенной для быстрого поиска нужной информации в перехваченных файлах.

Использовать для расчета необходимые статистические данные, взятые из конкретного банка, об имевших место ИИБ и количестве скопированных записей ПД, не представилось возможным, так как подобные сведения являются конфиденциальными. Поэтому в качестве возможного пути решения этой задачи выбрано использование внешних статистических данных. Однако в России отсутствует сколько-нибудь достоверная статистика о стоимости ПД и расходах, связанных с их раскрытием, поэтому пришлось обратиться к зарубежному опыту.

Среди публикаций, посвященных расчету стоимости утечек информации [20, 21], выделим [20], как одно из самых авторитетных и многократно цитируемых. В данной публикации собраны результаты исследований, проведенных в нескольких зарубежных странах[6] в 2018 году.

Согласно [20], стоимость одной записи ПД для финансовых учреждений стран, участвовавших в исследовании, составила в среднем 206$. Данная цифра получена с учетом всех прямых и косвенных расходов банков, к которым относятся следующие: обнаружение ИИБ, приведшего к утрате ПД; извещение клиентов, чьи записи были утрачены; выплата штрафов и компенсаций и т.д. Из представленных в работе данных можно получить, что в среднем за год на одну организацию-респондента приходилось по 24615 утраченных (утерянных или украденных) записей ПД.

Если предположить, что в банке за год будет утрачено упомянутое число записей ПД, то можно оценить среднее количество записей ПД, приходящееся на один ИИБ, выявляемый СКА до внедрения ПОРС

$$24615/43070 = 0{,}57.$$

Вычислив среднее число ИИБ, предотвращаемых в результате внедрения ПОРС в течение одного года,

$$43545 - 43070 \approx 475,$$

получим общее количество потенциально утрачиваемых за время нарушения функционирования СКА записей ПД

$$0{,}57 \cdot 475 = 271.$$

Умножив полученное число записей ПД на стоимость одной записи и на среднее значение курса доллара за 2018 год (1$ = 62,9 р.)[7] можно оценить стоимость для банка информации, утечку которой удалось бы предотвратить в течение года после начала использования ПОРС в связи с улучшением работы СКА, р.,

$$271 \cdot 206 \cdot 62{,}9 = 3511455.$$

Имея в своем распоряжении необходимую информацию, можно провести подобные рассуждения для других основных СЗИ, входящих в состав СМИИБ банка (антивирусное программное обеспечение, сканер безопасности, средство контроля портов ввода/вывода, межсетевой экран, система обнаружения атак [1, 2]), и получить оценку суммарной годовой выгоды для банка от использования ПОРС.

Отметим, что для оценки эффективности разработанного ПОРС также необходимо иметь сведения о затратах, связанных с выполнением исследовательских, проектных и внедренческих работ. Однако отсутствие таких сведений и ограниченный объем работы не позволили в настоящее время учесть данный фактор.

[6] В исследовании участвовали компании из США, Австралии, Великобритании, Германии, Франции, Бразилии, Японии, Италии, Индии, Объединенных Арабских Эмиратов и Саудовской Аравии.

[7] Среднее значение курса доллара получено как среднее арифметическое от всех значений ежедневного курса доллара США по отношению к российскому рублю, установленных Центральным банком России в 2018 году.

Выводы

1. Усовершенствована структура подсистемы обеспечения работоспособности, являющейся составной частью системы мониторинга инцидентов информационной безопасности, за счет введения блока оценки надежности средств защиты информации. Благодаря этой операции становится возможным определять по данным текущей эксплуатации вероятности состояния функционирования средств защиты информации, смена которых обусловлена нарушениями их работоспособности или устранением таких нарушений, и которые позволяют администратору безопасности более обоснованно принимать решения, связанные с обеспечением информационной безопасности автоматизированной банковской системы.

2. Определена структура и характеристики работы блока БОНСЗИ, с помощью которого оцениваются вероятности состояний функционирования каждого из СЗИ, входящего в состав СМИИБ, с использованием накапливаемых в процессе эксплуатации сведений о нарушениях в работе их компонентов.

3. Проведено, в качестве примера, сравнение результатов работы одного из СЗИ в составе СМИИБ, а именно средства контентного анализа, по критерию среднегодового числа ИИБ, выявляемых системой мониторинга до и после начала использования усовершенствованной ПОРС. Показано увеличение числа ИИБ, выявленных СКА в течение года, на 1,1 %, что соответствует для банка предотвращению экономических потерь в размере 3,5 млн рублей в год.

4. Усовершенствование работы ПОРС в составе СМИИБ позволило обеспечить более эффективный мониторинг инцидентов ИБ за счет повышения информированности администратора безопасности о текущем состоянии надежности средств защиты.

Список литературы

1. 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.

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

3. 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 : материалы 4-й Межвуз. науч.-практ. ежегодной конф., 13 мая 2011 г., Тамбов. – Тамбов, 2011. – С. 69 – 72.

4. Попов, С. В. Мониторинг состояний функционирования средств защиты информации в информационной системе / С. В. Попов, В. Н. Шамкин // Современные информационные технологии = «Contemporary Information Technologies» (Computer-Based Conference) : тр. Междунар. науч.-техн. конф., 2011 г., Пенза. – Пенза, 2011. – Вып. 13. – С. 165 – 168.

5. Попов, С. В. Определение вероятностей состояний функционирования средства контентного анализа как элемента системы мониторинга инцидентов информационной безопасности / С. В. Попов, В. Н. Шамкин // Вестн. Тамб. гос. техн. ун-та. – 2012. – Т. 18, № 1. – С. 27 – 37.

6. Попов, С. В. Алгоритм выявления инцидентов безопасности в информационной системе / С. В. Попов, В. Н. Шамкин // Всерос. науч. шк. «Актуальные проблемы нано- и микроэлектроники», 7–8 июля 2011 г., Тамбов. – Тамбов, 2011. – С. 223–224.

7. Попов, С. В. Методика мониторинга надежностных показателей средств защиты информации в банке по данным их текущей эксплуатации / С. В. Попов, В. Н. Шамкин // Вопр. соврем. науки и практики. Университет им. В. И. Вернадского. – 2012. – № 1 (37). – С. 54 – 65.

8. Запечников, С. В. Контроль целостности функциональных ресурсов средств защиты информации в распределенной среде / С. В. Запечников // Безопасность информационных технологий. – 2009. – Т. 16, № 1. – С. 37 – 44.

9. Fry, Ch. Security Monitoring / Ch. Fry, M. Nystrom. – O'Reilly, 2009. – 227 p.

10. Карповский, Е. Я. Надежность программной продукции / Е. Я. Карповский, С. А. Чижов. – Киев : Тэхника, 1990. – 160 с.

11. Запечников, С. В. Контроль целостности информационных ресурсов при распределенном хранении данных / С. В. Запечников // Безопасность информационных технологий. – 2008. – Т. 15, № 2. – С. 86 – 91.

12. Палюх, Б. В. Надежность программных средств экономических информационных систем: учеб. пособие / Б. В. Палюх, В. К. Кемайкин, А. Д. Дорожкин. – Тверь : Тверской гос. техн. ун-т, 2008. – 128 с.

13. Сердюк, В. А. Новое в защите от взлома корпоративных систем / В. А. Сердюк. – М. : Техносфера, 2007. – 360 с.

14. Badger, M. Zenoss Core Network and System Monitoring / M. Badger. – Birmingham : Packt Publising, 2008. – 261 p.

15. Hutton, N. Preparing for Security Event Management. – Текст : электронный / N. Hutton // 360 Information Security. – URL : http://www.windowsecurity.com/ uplarticle/NetworkSecurity/360is-prep-sem.pdf (дата обращения: 21.04.2020).

16. Swift, D. A Practical Application of SIM/SEM/SIEM Automating Threat Identification. – Текст : электронный / D. Swift // SANS Institute. – URL : http://www.sans.org/reading_room/ whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification_1781 (дата обращения: 21.04.2020).

17. Kocjan, W. Learning Nagios 3.0 / W. Kocjan. – Packt Publishing, 2008. – 316 p.

18. Olups, R. Zabbix 1.8 Network Monitoring / R. Olups. – Packt Publishing, 2010. – 428 p.

19. Wotring, B. Host Integrity Monitoring: Best Practises for Deployment. – Текст : электронный ресурс / B. Wotring // Security Focus. – URL : http://www.securityfocus.com/infocus/1771 (дата обращения: 21.04.2020).

20. Cost of Data Breach Study: Global Overview 2018. – Текст : электронный // IBM. – URL : https://www.ibm.com/downloads/cas/861MNWN2 (дата обращения: 21.04.2020).

21. Data Breach Investigations Report 2019. – Текст : электронный // Verizon. – URL : https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (дата обращения: 21.04.2020).

Improvement of the Information Security Subsystem in the Bank Information Security Monitoring System

D. Yu. Muromtsev[1], S. V. Popov[2], V. N. Shamkin[1]

Department of Design of Electronic and Microprocessor Systems (1), crems@mail.jesby.tstu.ru; TSTU, Tambov, Russia;
Department of Security and Information Technology (2), popovsvik@mpei.ru; National Research University "MPEI", Moscow, Russia

Keywords: reliability assessment unit; probabilities of state of functioning; information security; performance appraisal; health subsystem; information security tools.

Abstract: The paper describes of the subsystem for ensuring operability in the information security incident monitoring system, into which the unit for assessing the reliability of information protection means according to the current operation developed by the authors is introduced. The performance of the monitoring system was assessed before and after the start of using the improved subsystem to ensure operability.

References

1. Popov S.V., Shamkin V.N. [Factors affecting the effectiveness of monitoring information security incidents in an automated banking system], *Nauchno-tekhnicheskiy vestnik Povolzh'ya* [Scientific and Technical Bulletin of the Volga Region], 2010, no. 1, pp. 145-148. (In Russ., abstract in Eng.)

2. Popov S.V., Shamkin V.N. [On the influence of the functioning states of information security tools on the effectiveness of monitoring information security incidents in a bank], *Transactions of the Tambov State Technical University*, 2011, vol. 17, no. 2, pp. 297-303. (In Russ., abstract in Eng.)

3. Popov S.V., Shamkin V.N. *Novyye tekhnologii i innovatsionnyye razrabotki: materialy 4-y Mezhvuzovskoy nauchno-prakticheskoy yezhegodnoy konferentsii* [New technologies and innovative developments: materials of the 4th Interuniversity Scientific and Practical Annual Conference], 13 May, 2011, Tambov, 2011, pp. 69-72. (In Russ.)

4. Popov S.V., Shamkin V.N. *Sovremennyye informatsionnyye tekhnologii = «Contemporary Information Technologies» (Computer-Based Conference)* [Modern Information Technologies = "Contemporary Information Technologies" (Computer-Based Conference)], Proceedings International scientific and technical conference, 2011, Penza, 2011, issue 13, pp. 165-168. (In Russ.)

5. Popov S.V., Shamkin V.N. [Determination of the probabilities of the state of functioning of the content analysis tool as an element of the information security incident monitoring system], *Transactions of the Tambov State Technical University*, 2012, vol. 18, no. 1, pp. 27-37. (In Russ., abstract in Eng.)

6. Popov S.V., Shamkin V.N. *Vserossiyskaya nauchnaya shkola «Aktual'nyye problemy nano- i mikroelektroniki»* [All-Russian Scientific School "Actual Problems of Nano- and Microelectronics"], 7-8 July, 2011, Tambov, 2011, pp. 223-224. (In Russ.)

7. Popov S.V., Shamkin V.N. [Methodology for monitoring the reliability of indicators of information security in the bank according to their current operation], *Voprosy sovremennoy nauki i praktiki. Universitet im. V. I. Vernadskogo* [Problems of Contemporary Science and Practice. Vernadsky University], 2012, no. 1 (37), pp. 54-65. (In Russ., abstract in Eng.)

8. Zapechnikov S.V. [Integrity monitoring of the functional resources of information protection means in a distributed environment], *Bezopasnost' informatsionnykh tekhnologiy* [Security of information technologies], 2009, vol. 16, no. 1, pp. 37-44. (In Russ.)

9. Fry Ch. *Security Monitoring*, O'Reilly, 2009, 227 p.

10. Karpovskiy Ye.Ya., Chizhov S. A. *Nadezhnost' programmnoy produktsii* [Reliability of software products], Kiev: Tekhnika, 1990, 160 p. (In Russ.)

11. Zapechnikov S.V. [Control of the integrity of information resources during distributed data storage], *Bezopasnost' informatsionnykh tekhnologiy* [Security of information technologies], 2008, vol. 15, no. 2, pp. 86-91. (In Russ.)

12. Palyukh B.V., Kemaykin V.K., Dorozhkin A.D. *Nadezhnost' programmnykh sredstv ekonomicheskikh informatsionnykh sistem: uchebnoye posobiye* [Reliability of software tools of economic information systems: a training manual], Tver: Tverskoy gosudarstvennyy tekhnicheskiy universitet, 2008, 128 p. (In Russ.)

13. Serdyuk V.A. *Novoye v zashchite ot vzloma korporativnykh sistem* [New in protection against hacking of corporate systems], Moscow: Tekhnosfera, 2007, 360 p. (In Russ.)

14. Badger M. *Zenoss Core Network and System Monitoring*, Birmingham: Packt Publising, 2008, 261 p.

15. http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf (accessed 21 April 2020).

16. http://www.sans.org/reading_room/ whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification_1781 (accessed 21 April 2020).

17. Kocjan W. Learning Nagios 3.0, Packt Publishing, 2008, 316 p.

18. Olups R. Zabbix 1.8 Network Monitoring, Packt Publishing, 2010, 428 p.

19. http://www.securityfocus.com/infocus/1771 (accessed 21 April 2020).

20. https://www.ibm.com/downloads/cas/861MNWN2 (accessed 21 April 2020).

21. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (accessed 21 April 2020).

Verbesserung des Integritätssubsystems des Schutzes der Informationen im System der Überwachung der Vorfälle der Informationssicherheit bei der Bank

Zusammenfassung: Es ist die Beschreibung des Integritätssubsystems in dem System der Überwachung von Informationssicherheitsvorfällen, in das die von den Autoren entwickelte Einheit der Bewertung der Zuverlässigkeit der Mittel des Schutzes der Information gemäß dem aktuellen Betrieb eingeführt ist. Die Leistung des Überwachungssystems wurde vor und nach dem Beginn der Verwendung des verbesserten Subsystems bewertet, um die Funktionsfähigkeit sicherzustellen.

Perfectionnement du sous-système d'intégrité de la protection de l'information dans le système de surveillance des incidents de sécurité de l'information de la banque

Résumé: Est décrit le sous-système d'intégrité dans le système de surveillance des incidents de la sécurité de l'information, daans lequel est introduit une unité d'évaluation de la fiabilité des moyens de protection de l'information sur les données d'exploitation en cours élaborée par les auteurs. Le système de surveillance a été évalué avant et après l'utilisation du sous-système amélioré.

Авторы: ***Муромцев Дмитрий Юрьевич*** – доктор технических наук, профессор, проректор по научно-инновационной деятельности, ФГБОУ ВО «ТГТУ», г. Тамбов, Россия; ***Попов Сергей Викторович*** – кандидат технических наук, доцент кафедры безопасности и информационных технологий Инженерно-экономического института, ФГБОУ ВО «Национальный исследовательский университет «МЭИ», г. Москва, Россия; ***Шамкин Валерий Николаевич*** – доктор технических наук, профессор кафедры «Конструирование радиоэлектронных и микропроцессорных систем», ФГБОУ ВО «ТГТУ», г. Тамбов, Россия.

Рецензент: ***Алексеев Владимир Витальевич*** – доктор технических наук, профессор, заведующий кафедрой «Информационные системы и защита информации», ФГБОУ ВО «ТГТУ», г. Тамбов, Россия.