БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Atkina V.S.* Semantic model of disaster recovery information system // European Science and Technology: international scientific conference/ Bildungszentrum Rdk e.V. – Wiesbaden, Germany 2012. – P. 162-164.
2. *Машкина И.В. Сенцова А.Ю. Гузаиров Р.М. Кладов В.Е.* Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 25-35.
3. *Беленков В.Г. Будзко В.И. Синицын И.Н.* Катастрофоустойчивость корпоративных информационных систем. Ч. 1. – М.: ИПИ РАН, 2002.
4. *Будзко В.И.* Количественные оценки отказоустойчивых и катастрофоустойчивых решений // Вопросы защиты информации. – 2003. – № 2. – С. 19-32.
5. Аткина В.С. Живучесть системы как показатель ее катастрофоустойчивости // Проблемы обеспечения информационной безопасности в регионе : материалы III Регион. науч.-практ. конф., г. Волгоград, 20 апр. 2010 г. – Волгоград: Изд-во ВолГУ, 2010. – С. 42-57.
6. *Павлов А.Н. , Соколов Б.В.* Структурный анализ катастрофоустойчивой информационной системы //Труды СПИИРАН. Вып. 8. – М., 2009. – С. 128-153.
7. *Аткина В.С.* Подходы к оценке катастрофоустойчивости ИС// Проблемы модернизации региона в исследованиях молодых ученых: Материалы VI Межрегион. науч.-практ. конф., г. Волгоград, 30-31 марта 2010. – Волгоград: Изд-во ВолГУ, 2010. – С. 356-357.
8. *Литвиненко В.И., Дидык А.А., Фефелов А.А., Херсон.* Модифицированный гибридный иммунный алгоритм на основе теорий отрицательного и клонального отбора для решения задач классификации и его программная реализация // Моделирование информационных технологий. Вып. 62. – Киев, 2011. – С. 86-94.
9. *Зайцев С.А., Субботин С.А.* Обобщенная модель искусственной иммунной сети // Нейроинформатика. Ч. 2. – 2010. – С. 98-107.
10. Оладько А.Ю. Модель адаптивной многоагентной системы защиты в ОС Solaris 10 // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 210-217.
11. *Bidyuk P.I., Litvinenko V.I., Gasanov A.S.* Immune network based method for identification of turbine engine surging // Кафедра математического и системного анализа: [сайт]. URL – http://www.mmsa.kpi.ua. (дата обращения 10.09.2012).

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Аткина Владлена Сергеевна – Волгоградский государственный университет; e-mail: atkina.vlaldlena@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

Atkina Vladlena Sergeevna – Volgograd State University; e-mail: atkina.vlaldlena @ yandex.ru; 100, University avenue, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; senior lecturer.

УДК 004.942

Д.А. Ляшко, И.В. Аникин

МОДЕЛИРОВАНИЕ АГЕНТА И МЕНЕДЖЕРА СИСТЕМЫ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Целью работы является повышение эффективности защиты автоматизированных систем от несанкционированного доступа (НСД) за счет централизации управления функциями по защите информации от НСД. В работе определен состав компонентов и разработана структура системы централизованного удаленного администрирования средствами защиты информации от НСД (СУДАД-ЗИ), разработаны формальные математические

модели агента и менеджера, отвечающих за взаимодействие компонентов данной системы. Практическое использование предложенной структуры и математических моделей компонентов СУДАД-ЗИ позволяют осуществлять централизованное удаленное администрирование средств защиты информации от НСД и достичь поставленной цели.

Информационная безопасность; защита от несанкционированного доступа; удаленное управление.

D.A. Lyashko, I.V. Anikin

AGENT AND MANAGER MODELING FOR THE SYSTEM FOR REMOTE ADMINISTRATION OF UNAUTHORIZED ACCESS PROTECTION TOOLS

We suggested approach for increasing effectiveness of protection information systems from unauthorized access by centralization of controlling for protection functions. We suggested the structure of the system for remote administration of unauthorized access protection tools. We developed formal models for agent and manager for that system. These components are used for communication between components in it. We can use suggested structure and models for centralization of controlling our protection functions from unauthorized access.

Information security; protection from unauthorized access; remote control.

Защита от несанкционированного доступа (НСД) к информации является важнейшей задачей при проектировании автоматизированных систем (АС) в защищенном исполнении. При этом, в АС должны быть реализованы все необходимые требования РД ФСТЭК [1] в соответствии с требуемым классом защиты.

При проектировании системы защиты информации от несанкционированного доступа (СЗИ НСД) следует учитывать такие специфические признаки современных АС, как многоплатформенность, мультисервисность, территориальную распределенность, наличие большого количества пользователей, получающих доступ к значительному количеству ресурсов.

В таких условиях независимое администрирование отдельных средств защиты информации (СрЗИ) от НСД, присутствующих в АС, становится неэффективным и может привести к рассогласованию их конфигураций, увеличивает объемы работ по администрированию СрЗИ, количество ошибок администрирования, увеличивает общие затраты на построение СЗИ НСД. В связи с этим, для современных АС актуально использование систем централизованного удаленного администрирования СрЗИ от НСД (СУДАД-ЗИ), выполняющих удаленное администрирование и управление всеми функциями по защите информации в АС от НСД согласно требованиям ФСТЭК. Наличие такой СУДАД-ЗИ позволит повысить эффективность защиты АС.

Целью данной работы является повышение эффективности защиты АС от НСД за счет централизации управления функциями по защите информации.

Подходы к централизованному управлению функциями по защите информации в АС, в том числе по защите от НСД, исследовались в таких работах, как [2–7]. Ряд современных СЗИ НСД [8] предполагает централизацию управления и удаленное администрирование своими функциями по защите информации в рамках единых программных комплексов, однако до сих пор недостаточно хорошо проработана теоретическая база работы таких систем. В частности, недостаточно проработаны формализованные математические модели, определяющие структуру и функциональность таких систем, а также алгоритмы взаимодействия составляющих их компонентов. Таким образом, актуальность приобретает разработка такой теоретической базы, в частности *решение следующих задач*:

- определение состава компонентов и разработка структуры СУДАД-ЗИ;
- разработка формальных математических моделей для подсистем СУДАД-ЗИ.

Данная статья посвящена решению данных задач.

Характеристика рассматриваемых автоматизированных систем. Будем рассматривать в статье защиту от НСД АС класса 1В, представляющих многоплатформенные, мультисервисные, территориально распределенные сети со следующими особенностями:

- в АС могут использоваться автоматизированные рабочие места (АРМ), функционирующие под управлением различных операционных систем (ОС): в том числе Windows, а также сертифицированных ОС ИНТРОС, МСВС;
- в случае взаимодействия с внешними сетями, в АС используется межсетевое экранирование (МЭ);
- наряду с внутренними средствами защиты операционных систем, в АС могут использоваться используются иные СЗИ НСД, сертифицированные ФСТЭК;
- в АС присутствуют сервера баз данных;
- для решения задач резервного копирования информации, в АС существует сервер резервного копирования.

Таким образом, в рассматриваемых АС присутствует значительное количество разнотипных СрЗИ, требующих централизованного управления:

- внутренние СрЗИ НСД различных операционных систем;
- СрЗИ НСД, сертифицированные ФСТЭК;
- внутренние СрЗИ НСД серверов баз данных;
- СрЗИ межсетевых экранов.

Структура СУДАД-ЗИ. Наиболее удобным подходом для создания СУДАД-ЗИ является ориентирование на клиент-серверную архитектуру, а также применение системы программных агентов, устанавливаемых на администрируемые узлы, и управляемых с единой консоли администратора безопасности информации (АБИ). Данный подход наиболее часто применяется для централизованного управления решаемыми задачами в современных АС, в том числе для решения задач: резервного копирования информации, удаленного управления рабочими столами, удаленной печати, мониторинга событий в АС, обнаружения вторжений и атак в АС, контроля утечек информации из АС, в том числе и защиты от НСД. Выбрав данный подход, а также учитывая требования, предъявляемые к СЗИ НСД класса 1В, предлагается следующая структура СУДАД-ЗИ (рис. 1).

Компонентами СУДАД-ЗИ являются:

- Консоль АБИ.
- Менеджер.
- Агент.
- Программа взаимодействия с МЭ.
- Программа взаимодействия с ОС Windows и сертифицированными СЗИ НСД.
- Программа взаимодействия с сертифицированными ОС (в т.ч. ИНТРОС, МСВС).
- Программа управления резервным копированием.
- Программа взаимодействия с сервером БД.

Такая структура позволяет СУДАД-ЗИ осуществлять централизованное удаленное управление СЗИ НСД в рамках следующих подсистем:

- разграничения доступа;
- регистрации и учёта;
- обеспечения целостности;

- тестирования;
- мониторинга АС;
- антивирусного контроля.

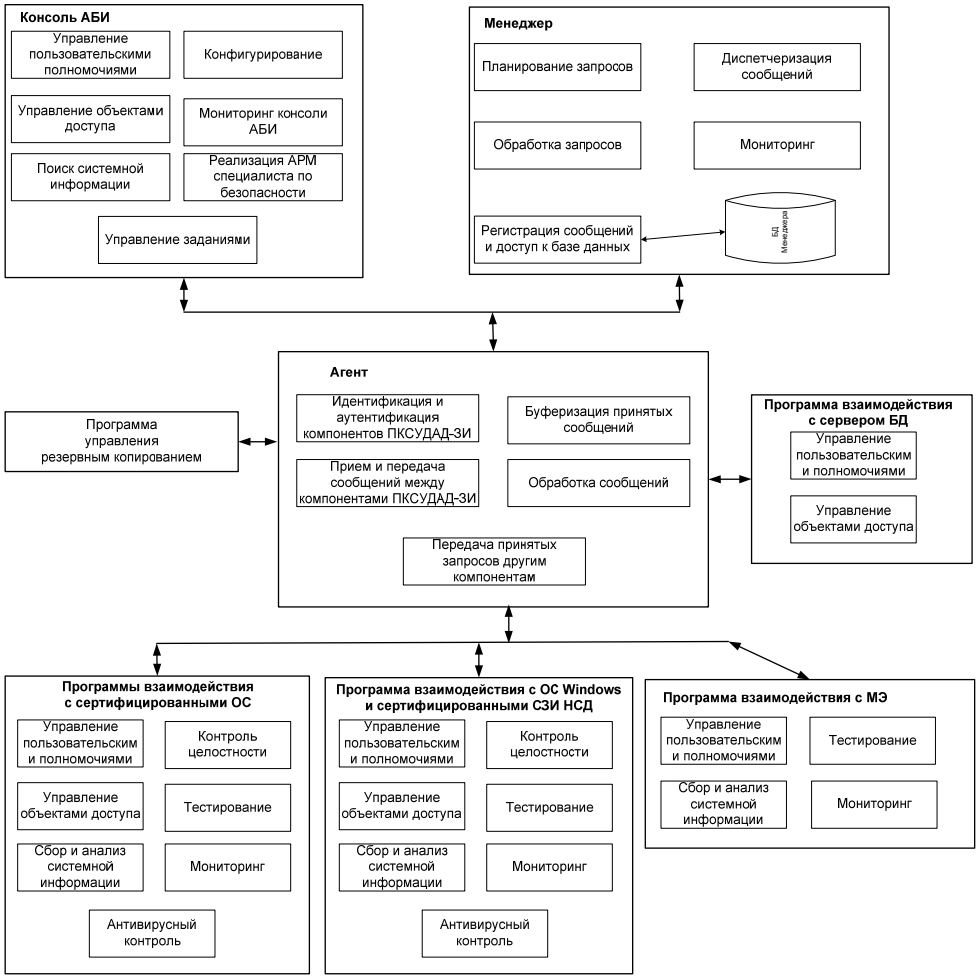

Рис. 1. Структура СУДАД-ЗИ

Графическая консоль АБИ используется АБИ для управления агентами и отображения текущего состояния АС. Менеджер предназначен для обработки и диспетчеризации запросов других компонентов СУДАД-ЗИ (Консоли АБИ, Агентов), мониторинга АС и регистрации событий, происходящих в АС. Агенты устанавливаются на администрируемые узлы и предназначены для организации взаимодействия между компонентами СУДАД-ЗИ путем обмена сообщениями.

Графическая консоль АБИ, Менеджер и Агенты являются основными компонентами СУДАД-ЗИ, через которые организуется удаленное администрирование и управление функциями по защите АС от НСД, а также взаимодействие всех компонентов СУДАД-ЗИ. В связи с этим, значительную актуальность приобретает разработка для них теоретической базы на уровне формальных и функциональных математических моделей.

Моделирование Агентов СУДАД-ЗИ

Предлагается следующая формальная модель **Агента:**

$$Agent = \langle Kernel, KLoader, Tlib, QT \rangle, \quad (1)$$

где $Kernel$ – ядро агента; $KLoader$ – загрузчик ядра агента; $Tlib$ – транспортная библиотека агента; QT – подсистема трансляции запросов.

Формальная модель *ядра Агента* представляется в следующем виде:

$$Kernel = \langle State, Q, Kernel\_Env, \{Agents\_Env\}, Enter\_Que \rangle,$$

где $State$ – состояние ядра агента, являющееся элементом множества состояний $\{инициализация, запуск\ и\ работа, останов, деинициализация\}$.

$Q = \langle Queue, events\_capacity, clients\_events\_everload, max\_peek\_count, deny\_m \rangle$ – окружение клиентов, с которыми взаимодействует агент, где $Queue = \langle Q = \{q_i\}, Q_n \rangle$ – структура данных типа «очередь» – очередь сообщений, которая используется для хранения сообщений, для клиента, при этом сообщения $q_i \in Q$ представляют собой тройки элементов $q_i = \langle context_i, content_i, sid_i \rangle$, где $context_i = \langle c_i, path_i = \{sid_{ij}\} \rangle$ – контекст сообщения, состоящий из двух частей: имени контекста c_i, маршрута передачи сообщения $path_i$, представляющего собой последовательность идентификаторов ядер агентов sid_{ij}, на которые пересылаются сообщения. $events\_capacity$ – максимальный набор хранимых в очереди сообщений; $clients\_events\_everload$ – нецелочисленный коэффициент превышения или занижения отведенного Агенту лимита объема сообщений в его очереди; max_peek_count – количество сообщений, которое Агенты могут запросить за один вызов; $deny\_m \in \{0,1\}$ – флаг, говорящий о том, будет ли получать Агент сообщения в свою очередь.

$Kernel\_Env$ – окружение ядра Агента, представляющее собой тройку элементов $\langle sid, authkey, xrtport, verbose, timeout, place \rangle$, где sid – уникальный строковый идентификатор ядра Агента; $authkey$ – ключ аутентификации для ядра Агента; $xrtport$ – номер TCP-порта для обслуживания запросов по сети; $verbose \in \{0,1\}$ – необходимость протоколирования внутренней работы ядра; $timeout$ – таймаут удерживания простаивающего соединения в открытом режиме; $place$ – место назначения, используемое при передаче файлов между Агентами.

$Agents\_Env$ – окружение соседних агентов, представляющее собой пятерку элементов $\langle sid, authkey, ip, ip\_dup, xrtport, traffic\_\lim it \rangle$, где sid – уникальный строковый идентификатор соседнего Агента; $authkey$ – ключ аутентификации для соседнего Агента; ip – основной IP-адрес соседнего Агента; ip_dup – дублирующий IP-адрес (если существует) соседнего Агента; $xrtport$ – номер TCP-порта для обслуживания запросов по сети; $raffic\_\lim it$ – положительное число указывает ограничение скорости передачи данных в байтах в секунду для Агента.

$Enter\_Que = \{addr_i\}$ – точки входа для обработки агентом запросов.

Загрузчик ядра агента *KLoader* представляет собой сервис, предназначенный для проведения предварительных работ перед загрузкой Ядра Агента и непосредственно для загрузки Ядра Агента. Загрузчик ядра Агента запускается при загрузке ОС.

Транспортная библиотека агента Tlib обеспечивает взаимодействие клиента с ядром Агента и предоставляет интерфейс для отправки и получения клиентами сообщений.

Подсистема трансляции запросов предназначена для приема сообщений и передачи их для обработки программам взаимодействия с администрируемыми СЗИ. Она выполняет следующие действия: прием сообщения для трансляции, синтаксический разбор сообщения, анализ и передача управления программам взаимодействия, обрабатывающим соответствующее сообщение, прием результата выполнения операции и отправка результата отправителю сообщения.

При работе ядра Агента можно выделить несколько состояний, каждое из которых имеет определенные характеристики, описывающие процесс. Состояние ядра агента описывается элементом *State* модели (1) и может являться одним из следующих: инициализация; запуск и работа; останов; деинициализация.

На рис. 2 представлена функциональная модель работы ядра Агента СУДАД-ЗИ через последовательную схему его состояний.

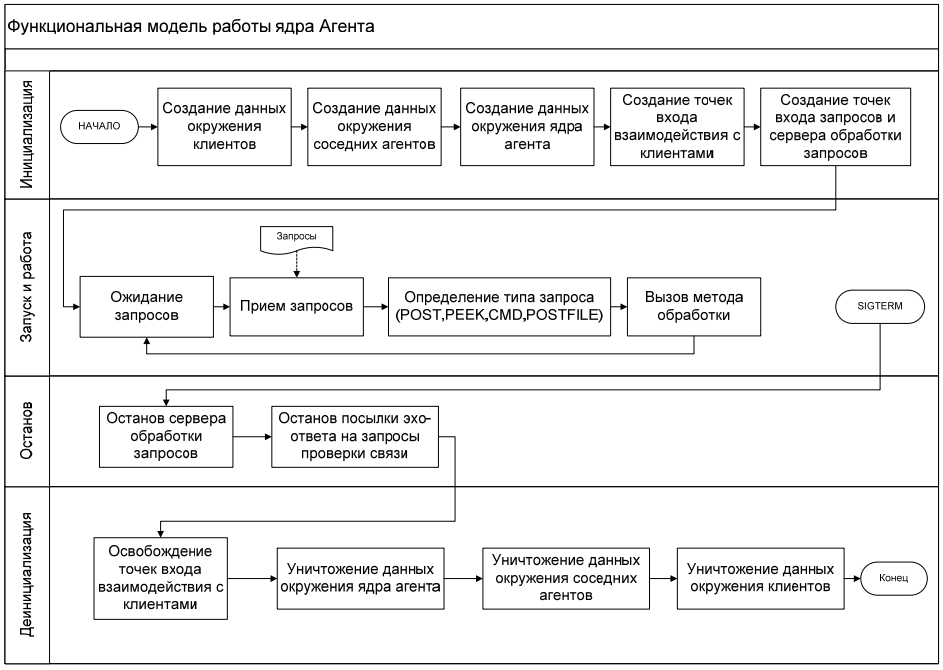

Рис. 2. Функциональная модель работы ядра Агента

Моделирование Менеджера СУДАД-ЗИ. Работа Менеджера заключается в управлении взаимодействием четырёх самостоятельных, одновременно выполняющихся процессов (планирование запросов, обработка сообщений, мониторинг, регистрация событий) с потоками входящих сообщений, базой данных и очередью исходящих сообщений. Передача сообщений от Менеджера к Агентам выполняется в виде заданий через очередь исходящих сообщений.

Задание представляет собой единицу работы в СУДАД-ЗИ, формальная модель которого представляется в виде:

$Job = \langle JobName, Start\_Condition, Date, Time, Configuration, Report, completed, result \rangle$,

где $JobName$ – имя задания; $Start\_Condition$ – периодичность запуска задания $\in \{ежемесячно, еженедельно, ежедневно\}$; $Date$ – дата запуска; $Time$ – время запуска; $Configuration = \langle type, h\_id, name, Items, Initialized \rangle$ – конфигурация задания, где $type$ – тип задания (контроль целостности, резервное копирование, тестирование, антивирусный контроль), h_id – идентификатор администрируемой СЗИ, $name$ – имя конфигурации, $Items$ – элементы конфигурации (например, параметры командной строки), $Initialized \in \{0,1\}$ – признак инициализации; *Report* – отчет о выполнении задания; $Completed$ – время завершения выполнения; $\mathrm{Re}sult \in \{0,1\}$ – результат выполнения.

Записи системного журнала в БД Менеджера представляются в виде следующего кортежа:

$$event = \langle etype, atype, rtype, date, time, agent\_id, stype, subject, object, desc \rangle,$$

где *etype∈{Неопределенный тип, Деятельность субъекта доступа, Изменение состояния процесса субъектом доступа, Доступ процесса к локальным ресурсам, Доступ процесса к каналам связи, Изменение прав доступа субъектом доступа, Попытка НСД, Системное событие}* – идентификатор типа события; *atype∈{Неопределенный тип, Загрузка, Активизация, Деактивизация, Чтение, Запись, Создание, Удаление}* – идентификатор типа деятельности; *rtype∈{Неопределенный тип, Успех, Неудача, Частичный успех, Системная ошибка, Информационное сообщение}* – идентификатор типа результатов деятельности; *date* – дата события; *time* – время события; *agent_id* – идентификатор агента; *stype∈{ОС Windows, INTROS, МСВС, МЭ, BD}* – идентификатор типа администрируемой СЗИ; *subject* – субъект; *object* – объект; *desc* – описание события.

Функциональная схема работы менеджера представлена на рис. 3.

В ходе мониторинга, выполняемого Менеджером, осуществляется также обнаружение попыток НСД через определение наличия на узлах незарегистрированных пользователей. Такие пользователи могут быть созданы злоумышленником в обход авторизованных механизмов, например, через получение злоумышленником удаленной командной строки к узлу, используя уязвимости ОС.

На базе разработанных формальных и функциональных моделях авторами разрабатывается программный комплекс СУДАД-ЗИ для обеспечения удаленного администрирования СЗИ НСД в АС класса 1В.

Выводы. Практическое использование предложенной структуры и математических моделей компонентов СУДАД-ЗИ позволяют осуществлять централизованное удаленное администрирование СрЗИ НСД. Такая централизация позволит во многом повысить эффективность зашиты информации от НСД за счет:

- обеспечения гибкости и управляемости политики информационной безопасности (ИБ) в АС в области защиты от НСД;
- повышения уровня защищенности АС за счет согласования конфигураций различных СрЗИ НСД;
- снижения количества операций, выполняемых администратором безопасности информации (АБИ) в АС;
- снижения количества ошибок администрирования АС;
- наличия единого комплекса администрирования СрЗИ, что позволит сократить количество технических средств в АС.

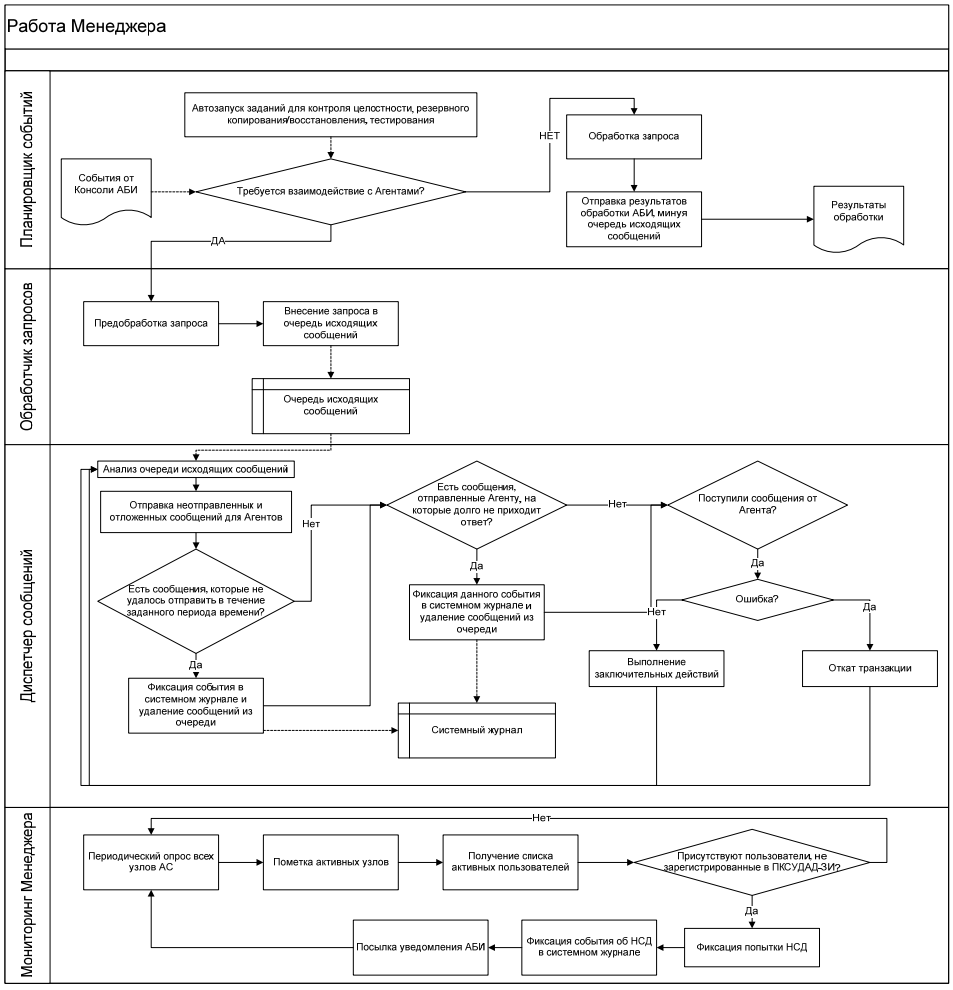

Рис. 3. Функциональная схема работы менеджера

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гостехкомиссия России. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». – М., 1992.
2. *Зегжда Д.П., Калинин М.О., Москвин Д.А.* Повышение эффективности администрирования безопасности информационных систем путем управления параметрами программных средств контроля доступа // Материалы XVII научно-технической конференции «Методы и технические средства обеспечения безопасности информации». – СПб., 2008. – С. 21.
3. *Васильев В.И.* Интеллектуальные системы защиты информации: Учеб. пособие. – М.: Машиностроение, 2010. – 152 с.
4. *Котенко И.В., Уланов А.В.* Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети Интернет // Известия РАН. Теория и системы управления. – 2007. – № 5. – С. 74-88.
5. *Хади Р.А.* Разработка архитектуры программной системы конфиденциального доступа к информационным ресурсам электронно-вычислительных сетей: Дисс. … канд. техн. наук. – Ростов-на-Дону, 2003. – 160 с.
6. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004 – 384 с.

7. *Конявский В.А.* Управление защитой информации на базе СЗИ НСД «АККОРД». – М.: Радио и связь, 1999. – 325 с.
8. *Веретенников А.А.* Развертывание СЗИ НСД Secret Net в корпоративной сети с использованием протокола RDP, функции автоматической установки клиента и удаленной установки программного обеспечения аппаратной поддержки» // [Электронный ресурс] http://www.itsecurity.ru/press/pdf/Secret_Net_deployment_with_RDP.pdf.

Статью рекомендовал к опубликованию д.т.н., профессор И.И. Исмагилов.

Ляшко Дмитрий Анатольевич – ОАО «АйСиЭл – КПО ВС»; email: dimal@icl.kazan.ru; 420111, г. Казань, Сибирский тракт, 10; тел.: 89872964027; технический директор; соискатель.

Аникин Игорь Вячеславович – Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ; email: anikinigor777@mail.ru; 420073 г. Казань, ул. Гвардейская, 24-45; тел.: 89520421458; кафедра систем информационной безопасности; зав. кафедрой; к.т.н.; доцент.

Lyashko Dmitriy Anatol'evich – ICL-KME CS; email: dimal@icl.kazan.ru; 10, Siberian road, Kazan', 420111, Russia; phone: +79872964027; technical director; competitor.

Anikin Igor Vyacheslav'ovich – Kazan State Technical University named after A.N. Tupolev-KAI; email: anikinigor777@mail.ru; 24-45, Gvardeyskayu street, Kazan', 420073, Russia; phone: 89520421458; the department of information security; head the department; cand. of eng. sc.; associate professor.

УДК 004.056.5 004.89

А.А. Бешта

АРХИТЕКТУРА АГЕНТА КОНТРОЛЯ НАД ВНУТРЕННИМ ЗЛОУМЫШЛЕННИКОМ НА ОСНОВЕ МЕХАНИЗМА ОЦЕНКИ ДОВЕРИЯ

Целью данного исследования является разработка архитектуры агента контроля над внутренним злоумышленником на основе механизма оценки доверия. В рамках данного исследования была предложена методика оценки доверия к наблюдаемому объекту на основе поданных за объект голосов с учетом важности этих голосов, для этого разработана (ε; θ) – доверительная модель объекта. Показано влияние коэффициентов модели на уровень доверия и предложены управляющие параметры модели. На основе этой модели построен алгоритм контроля над внутренним злоумышленником. Предложена архитектура программного агента, реализующая данный алгоритм. Показаны основные модули агента и составляющие их блоки, описаны информационные потоки между ними, описаны основные функции всех блоков и логика работы агента.

Внутренний злоумышленник; деструктивное воздействие; доверие к объекту; событие информационной системы.

A.A. Beshta

ARHITECRURE OF INSADERS CONTROL AGENT BASED ON CONFIDENCE EVALUATION APPROACH

The purpose of the research is development of architecture of control over insiders agent based on object confidence evaluation approach. In this research the method of confidence evaluation to observed object was proposed. This method account voices for observed object and their importance. For this purpose (ε; θ) – object confidence model was developed. Influence of model's factors on confidence level was shown and control parameters of model were developed. Algo-