УДК 004.942

СТРУКТУРА И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ КОМПОНЕНТОВ СИСТЕМЫ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

[1]Ляшко Д.А., [2]Аникин И.В.

[1]ОАО «АйСиЭл – КПО ВС», Казань, email: dimal@icl.kazan.ru;

[2]ФГБОУ ВПО «Казанский национальный исследовательский технический университет им. А.Н. Туполева», Казань, email: anikinigor777@mail.ru

Разработана структура системы удаленного администрирования средствами защиты информации от НСД (СУДАД-ЗИ), определены состав и функции ее компонентов. Разработаны теоретико-множественные и функциональные модели агента и менеджера, отвечающих за взаимодействие компонентов данной системы. Разработан программный комплекс для удаленного администрирования средствами защиты информации от НСД. В качестве защищаемых автоматизированных систем рассматриваются многоплатформенные, мультисервисные и территориально распределенные сети. Программный комплекс позволяет управлять средствами защиты информации от НСД различных операционных систем, межсетевых экранов, серверов БД. Практическое применение разработанного программного комплекса позволяет повысить эффективность защиты информации от НСД за счет обеспечения гибкости и управляемости политики информационной безопасности, согласования конфигураций различных средств защиты информации от НСД, снижения количества операций, выполняемых администратором безопасности информации, снижения количества ошибок администрирования.

Ключевые слова: информационная безопасность, защита от несанкционированного доступа, удаленное управление

STRUCTURE AND COMPONTNT'S MODELLING FOR A SYSTEM OF REMOTE ADMINISTRATION OF UNAUTHORIZED ACCESS PROTECTION TOOLS

[1]Lyashko D.A., [2]Anikin I.V.

[1]OJC ICL KMO-CS, Kazan, email: dimal@icl.kazan.ru;

[2]Kazan National Research Technical University, Kazan, email: anikinigor777@mail.ru

We have suggested a structure for a system of remote administration of unauthorized access protection tools (SUDAD-ZI), list of components and their functions also have been suggested. We have developed formal models for agent and manager for SUDAD-ZI. Agent and manager are using for interaction between other components in SUDAD-ZI. We have developed the software for remote administration of unauthorized access protection tools. This software can be used for protection computer networks from unauthorized access. We can use this software to protect multiplatform, distributed computer networks with many IT-services. Developed software can be used to control access protection tools in operating systems, firewalls, database servers. We have increased effectiveness of protection from unauthorized access with using developed software by increasing flexibility of security policy, configuration consistent, decreasing number of operation of security administrator, decreasing number of mistakes of security administration.

Keywords: information security, protection from unauthorized access, remote control

Защита от несанкционированного доступа (НСД) к информации является одной из важнейших задач при проектировании автоматизированных систем (АС) в защищенном исполнении. При этом, защита должна строиться на основании требований нормативных документов [1], учитывая такие специфические признаки современных АС, как многоплатформенность, мультисервисность, территориальная распределенность. В данных условиях независимое администрирование отдельных средств защиты информации (СрЗИ) от НСД, защищающих компоненты АС, становится неэффективным и увеличивает общие затраты на построение системы защиты информации от НСД (СЗИ НСД). В связи с этим, для современных АС становится актуально использование систем централизованного удаленного администрирования СрЗИ от НСД (СУДАД-ЗИ).

Подходы к централизованному управлению функциями по защите информации в АС, в том числе по защите от НСД, исследовались в таких работах, как [2–8]. Тем не менее, до сих пор недостаточно хорошо проработана теоретическая база для таких систем, в частности формализованные математические модели, определяющие структуру и функциональность таких СЗИ НСД, а также механизмы взаимодействия составляющих их компонентов.

Целью данного исследования является разработка теоретических положений для создания СУДАД-ЗИ, позволяющих осуществлять централизацию управления своими функциями по защите информации. Применение такой СУДАД-ЗИ позволит повысить эффективность защиты АС от НСД за счет централизации управления.

Данная статья посвящена решению следующих задач, направленных на дости-

жение цели исследования: определение состава компонентов и разработка структуры СУДАД-ЗИ, разработка формальных математических моделей для ее подсистем, разработки программного комплекса СУДАД-ЗИ.

Структура СУДАД-ЗИ

В статье рассматривается защита от НСД АС класса 1В, включающих в себя 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. Наиболее удобным подходом для создания системы их централизованного администрирования 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 рамках данного подхода, а также учитывая требования, предъявляемые к СЗИ НСД класса 1В [1], предлагается следующая структура СУДАД-ЗИ (рис. 1).

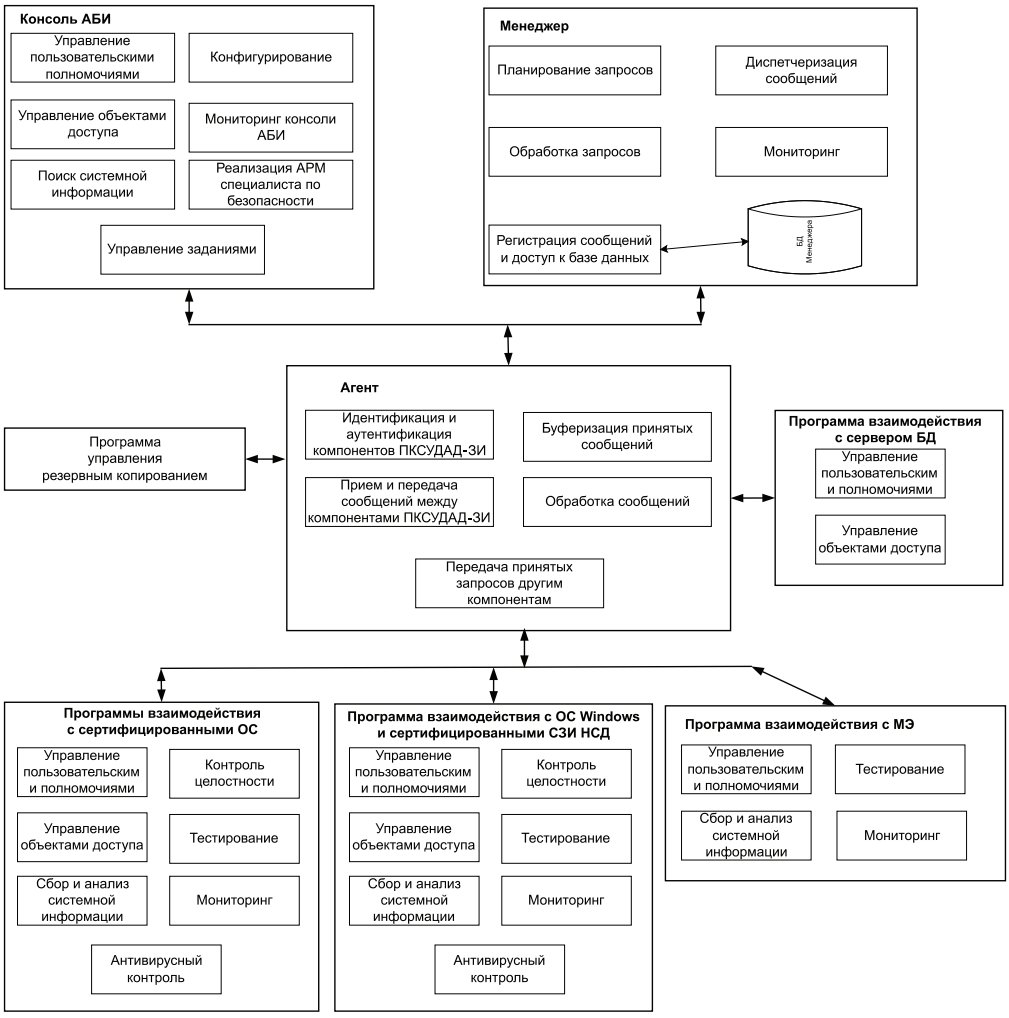

Рис. 1. Структура СУДАД-ЗИ

Предложенная структура СУДАД-ЗИ позволяет осуществлять централизованное удаленное управление СЗИ НСД в рамках подсистем разграничения доступа, регистрации и учёта событий, обеспечения целостности, тестирования, мониторинга АС, антивирусного контроля. При этом назначение графической консоли АБИ заключается в управлении агентами и отображении 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. Менеджер и агенты являются основными компонентами СУДАД-ЗИ, через которые организуется удаленное администрирование и управление функциями по защите АС от НСД. В связи с этим, значительную актуальность приобретает разработка для них формальных математических моделей.

Моделирование агентов СУДАД-ЗИ

Предлагается следующая формальная модель агента:

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

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

Формальная модель *ядра Агента* представляется в следующем виде:

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

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 $context_i = \langle c_i, parth_i = \{sid_{ij}\} \rangle$ – 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 ⟨*sid*, *authkey*, *xrtport*, *verbose*, *timeout*, *place*⟩, 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 шестерку элементов ⟨*sid*, *authkey*, *ip*, *ip_dup*, *xrtport*, *traffic*_lim *it*⟩, 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; *traffic*_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.

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

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 ∈ {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* ∈ {0, 1} – признак инициализации; *ReportReport* – отчет о выполнении задания; *Completed* – время завершения выполнения; *Result* ∈ {0, 1} – результат выполнения.

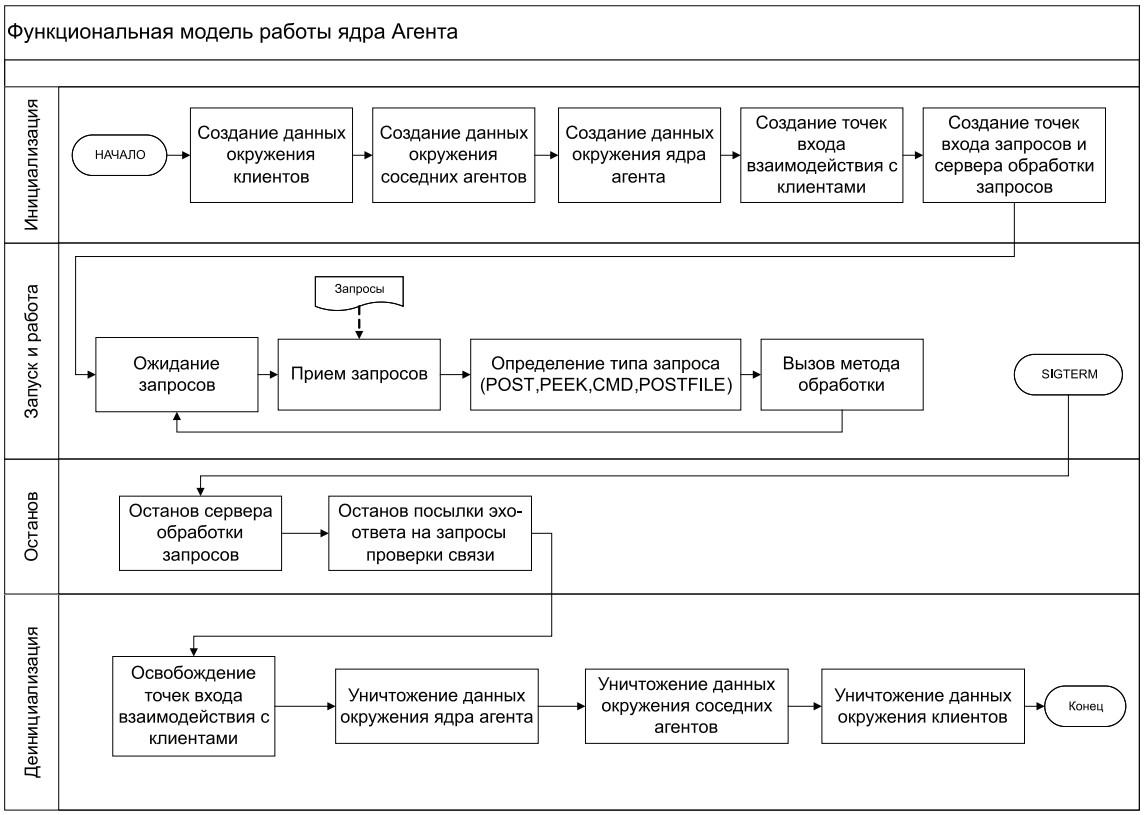

Рис. 2. Функциональная модель работы ядра Агента

Регистрация и учет событий, происходящих в АС, осуществляется в системном журнале базы данных Менеджера. В нем осуществляется централизация регистрационной информации, доступ к которой возможно получить с графической консоли АБИ. В данном журнале осуществляется и фиксация попыток НСД в АС, реализуемая подсистемой мониторинга. 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.

Программный комплекс СУДАД-ЗИ

На основании вышепредложенных моделей авторами разработан программный комплекс СУДАД-ЗИ, который реализует множество функций по защите информации от НСД (таблица).

В качестве примера на рис. 3. представлены этапы формирования задания, связанного с антивирусным контролем.

Функции, реализуемые подсистемами ПКСУДАД-ЗИ

Подсистема	Функции ПКСУДАД-ЗИ
Управление доступом	Создание/удаление/изменение полномочий пользователей
	Блокирование/разблокирование пользовательских полномочий
	Генерирование/выдача парольной информации
	Формирование/перезапись аппаратных ключей идентификации для системы контроля и разграничения доступа и сертифицированных СрЗИ
	Управление начальной конфигурацией СрЗИ на узлах сети
	Создание/модификация дискреционных прав доступа к защищаемым ресурсам
	Создание/модификация мандатных прав доступа к защищаемым ресурсам
Регистрация и учет событий	Просмотр информации систем регистрации и учета
	Поиск в данных регистрации и учета с возможностью задания критериев поиска по всем значимым полям регистрационных и учетных записей
	Полнотекстовый поиск в регистрационных и учетных записях
	Регистрация и учет событий, связанных с выводом документов на печать.
Мониторинг АС	Получение оперативной информации о попытках НСД
	Блокировка/Разблокировка АРМ нарушителя
	Генерация отчета о критичных событиях за выбранный период времени
Обеспечение целостности	Создание/модификация/удаление конфигурационных файлов контроля целостности
	Привязка конфигурационных файлов к проверяемым объектам
	Запуск процессов контроля целостности на проверяемых объектах
	Просмотр результатов контроля целостности
	Резервное копирование информации
Тестирование	Запуск тестов СрЗИ
	Просмотр результатов тестирования СрЗИ
Антивирусный контроль	Запуск заданий по антивирусному контролю
	Просмотр отчетов
	Обновление антивирусных баз

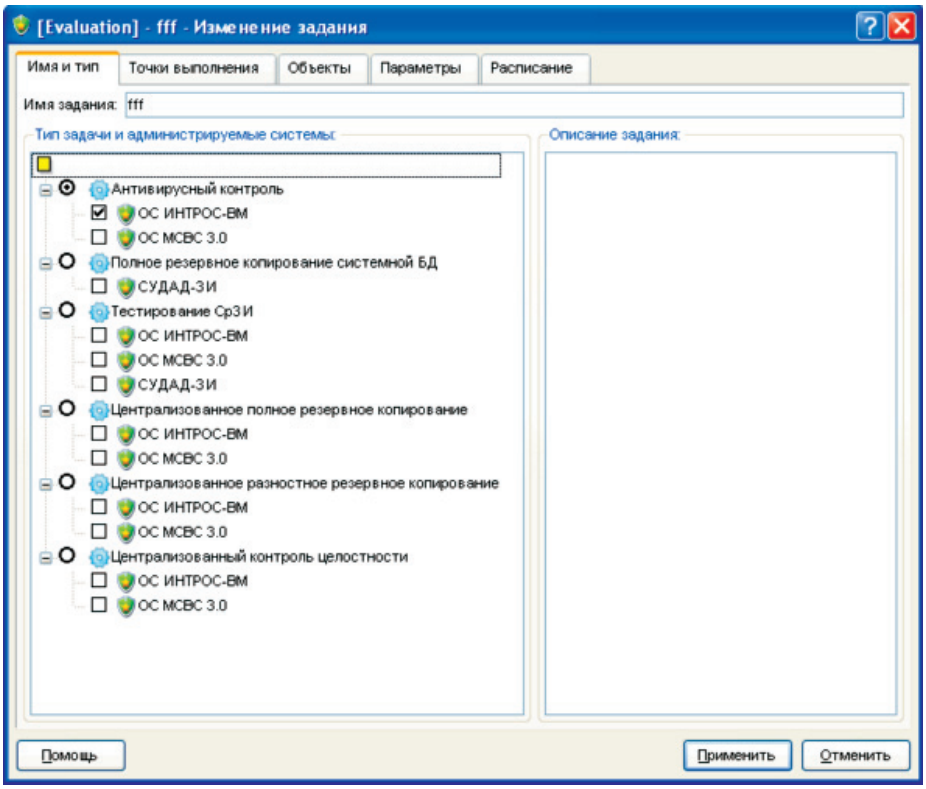

Рис. 3. Формирование заданий в ПКСУДАД-ЗИ

Применение ПКСУДАД-ЗИ позволяет повысить эффективность защиты от НСД многоплатформенных, мультисервисных, территориально распределенных АС путем централизации управления функциями по защите информации. Эффективность достигается за счет:

– повышения уровня защищенности за счет согласования основных параметров различных СрЗИ;

– снижения количества операций выполняемых администратором безопасности информации (АБИ);

– снижения количества ошибок администрирования СрЗИ;

– централизации регистрационной информации, что позволяет проводить более глубокий анализ работы СрЗИ изделия в целом и своевременно выявлять угрозы безопасности информации;

– введения единого бюджета пользователя для доступа ко всем системам, что позволяет уменьшить ошибки пользователя;

– введения единого комплекса администрирования СрЗИ, что позволяет сократить количество технических средств СЗИ НСД в АС.

Выводы

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

Список литературы

1. 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.

2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: руководящий документ // Гостехкомиссия России. – М., 1992.

3. Зегжда Д.П. Повышение эффективности администрирования безопасности информационных систем путем управления параметрами программных средств контроля доступа / Д.П. Зегжда, М.О. Калинин, Д.А. Москвин // Методы и технические средства обеспечения безопасности информации: материалы XVII научно-технической конференции. – СПб., 2008. – С. 21.

4. Интеллектуальные системы защиты информации: учеб. пособие / В.И. Васильев. – М.: Машиностроение, 2010. – 152 с.

5. Конявский В.А. Управление защитой информации на базе СЗИ НСД «АККОРД» – М.: Радио и связь, 1999. – 325 с.

6. Котенко И.В. Многоагентное моделирование защиты информационных ресурсов компьютерных сетей в сети интернет / И.В. Котенко, А.В. Уланов // Известия РАН. Теория и системы управления. – 2007. – № 5. – С. 74–88.

7. Хади Р.А. Разработка архитектуры программной системы конфиденциального доступа к информационным ресурсам электронно-вычислительных сетей: дис. ... канд. техн. наук. – Ростов на Дону, 2003. – 160 с.

8. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

References

1. Veretennikov Aleksandr Anatol’evich «Razvertyvanie SZI NSD Secret Net v korporativ-noj seti s ispol’zovaniem protokola RDP, funkcii avtomaticheskoj ustanovki klienta i udalen-noj ustanovki programmnogo obespechenija apparatnoj podderzhki» // http://www.itsecurity.ru/press/pdf/Secret_Net_deployment_with_RDP.pdf.

2. Gostehkomissija Rossii. Rukovodjashhij dokument «Avtomatizirovannye sistemy. Zashhita ot nesankcionirovannogo dostupa k informacii. Klassifikacija avtomatizirovannyh sistem i trebovanija po zashhite informacii». Moskva, 1992.

3. Zegzhda D.P. Povyshenie jeffektivnosti administrirovanija bezopasnosti informacion-nyh sistem putem upravlenija parametrami programmnyh sredstv kontrolja dostupa / Zegzhda D.P., Kalinin M.O., Moskvin D.A. // Materialy XVII nauchno-tehnicheskoj konferencii «Metody i tehnicheskie sredstva obespechenija bezopasnosti informacii». SPb, 2008. pp. 21.

4. Intellektual’nye sistemy zashhity informacii: ucheb. posobie / V.I. Vasil’ev. M.: Mashinostroenie, 2010. 152 p.

5. Konjavskij V.A. Upravlenie zashhitoj informacii na baze SZI NSD «AKKORD» M.: Radio i svjaz’, 1999. 325 p.

6. Kotenko I.V. Mnogoagentnoe modelirovanie zashhity informacionnyh resursov komp’juternyh setej v seti Internet / I.V. Kotenko, A.V. Ulanov // Izvestija RAN. Teorija i sistemy upravlenija. 2007. no. 5. pp. 74–88.

7. Hadi R.A. Razrabotka arhitektury programmnoj sistemy konfidencial’nogo dostupa k informacionnym resursam jelektronnovychislitel’nyh setej // Dissertacija na soiskanie uche-noj stepeni kandidata tehnicheskih nauk. Rostov na Donu, 2003. 160 p.

8. Shheglov A.Ju. Zashhita komp’juternoj informacii ot nesankcionirovannogo dostupa. SPb.: Nauka i tehnika, 2004 384 p.

Рецензенты:

Песошин В.А., д.т.н., профессор, заведующий кафедрой компьютерных систем Казанского национального исследовательского технического университета им. А.Н. Туполева, КАИ, КНИТУ-КАИ, г. Казань;

Кузнецов В.М., д.т.н., профессор, профессор кафедры компьютерных систем Казанского национального исследовательского технического университета им. А.Н. Туполева, КАИ, КНИТУ-КАИ, г. Казань.

Работа поступила в редакцию 22.02.2013.