УДК 004.056

ФУНКЦИОНАЛЬНАЯ СТРУКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЛЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Ф.П.АЛИЕВА
Бакинский Государственный Университет
aaliyev@mail.ru

В статье предложена функциональная структура системы обеспечения безопасности. А также приведены основные функции, изложены принципы и порядки действия, описаны основные функциональные модули системы обеспечения безопасности.

Ключевые слова: система безопасности, система обеспечения безопасности, функции системы безопасности, модули системы безопасности

Методы и средства обеспечения безопасности объектов (ресурсов и компонентов) сети разделяют на локальные и сетевые средства защиты. Локальные средства обеспечения безопасности реализуются в составе абонентских систем, и предназначены для проверки прав доступа абонентов к ресурсам. Под сетевыми средствами понимают средства, обеспечивающие управление потоками защищаемых ресурсов и данных в сети, а также средства, выполняющие свои функции в тесном взаимодействии с процессами управления передачи данных [1-3].

Предполагается, что система обеспечения безопасности (СОБ) должна иметь, по крайней мере, одно средство для защиты объектов на каждом пути доступа к ним или проникновения в систему. Поэтому в концептуальной модели СОБ точно определяется каждая область сети, требующая защиты и оценивается эффективность средств защиты.

СОБ в компьютерной сети (КС) реализуется на высоком уровне эталонной модели и является самым верхним компонентом в системной иерархии. СОБ, как правило, состоит из нескольких модулей, которые выполняют следующие функции [3,4]:

- управление входом пользователей в систему (УВП);
- управление доступом к системе и ее ресурсам (УДС);
- учет и регистрация входов и обращений к системе (УРВ);
- аутентификация пользователя и сети (АПС);

- управление правами и полномочиями пользователей (УПП);
- непосредственная защита информации (НЗИ);
- генерация и распространение ключами (ГРК);
- обеспечение целостности (ОЦ);
- установление подлинности данных (УП);
- анализ состояния и контроля угроз (АС);
- отключение системы (ОС);
- реорганизация и реконфигурирования системы (РРС).

Каждый пользователь должен войти в систему через УВП, который выдает общую справку о системе. После чего пользователю предоставляется возможность представить свой ID и пароль (PSWD). После этого управление передается в УДС, который принимает от пользователя эти параметры и проверяет санкционирование доступа к системе и требуемым ресурсам. В случае обнаружения несанкционированного доступа (НСД) он выдает пользователю сообщение об отказе. При положительном результате управление передается в УРВ, который регистрирует все входы и обращения к системе и к ее ресурсам. В случае несанкционированного доступа регистрируется несанкционированное обращение к системе в журнале нарушений.

АПС с помощью дополнительной процедуры проводит аутентификацию и устанавливает подлинность пользователя. Кроме того, АПС позволяет пользователю определить подлинность сети или системы. Если не устанавливается подлинность пользователя и сети, то управление передается в УРВ, иначе - в УПП, которое получив управление, следит за работой пользователей. Для определения полномочий и привилегий используется двухмерная матрица $A=\{a_{ij}\}$, $i=\overline{1,n}$, $j=\overline{1,m}$, где n - количество пользователей, m - количество ресурсов сети. Коэффициент, который стоит на пересечение строки i и столбца j, определяет категории доступа i-го пользователя j-му ресурсу.

НЗИ защищает данные от несанкционированного использования, как при хранении, так и при передаче, для чего используются криптографические и стенографические методы. Каждый раз при передаче по сети или при любом криптографическом сокрытии информации управление передается в НЗИ.

Передача информации производится по специальному протоколу СОБ, согласно которому каждый пользователь имеет два ключа - один открытый, другой секретный. Открытый ключ печатается открыто и используется другими пользователями для шифрования информации, которая предназначена для данного пользователя. Секретный ключ известен только пользователю - владельцу и используется для расшифровки. Ключи генерируются и сохраняются в центре распределения ключей (ЦРК).

Работа ЦРК регулируется ГРК, который кроме генерации и сохранения ключей, также выполняет функции замены устаревших ключей, обмен ключами между пользователями, передача ключей пользователям из ЦРК.

УП получает управление из НЗИ и ГРК, которое обеспечивает проверку целостности и подлинности информации. В положительном случае к НЗИ и ГРК возвращается удовлетворительное сообщение, и они продолжают свою работу, в обратном случае выдается сообщение о нарушении.

Функции АС распадаются на несколько направлений: диагностика, обеспечение надежного функционирования, выявление угроз и нарушений. Первая часть запускается в случае появления любого сообщения о НСД в систему или к ее ресурсам, о нарушении и т.д. Ведутся диагностика контроля входов пользователей в систему, таблицы полномочий и привилегий. Вторая часть, т.е. подсистема обеспечения надежного функционирования, контролирует все модули и процедуры системы безопасности. В случае отказа какого-либо элемента системы безопасности, выдается сообщение администратору СОБ и по необходимости передается управление в модуль РРС. Третья часть проводит мероприятия для выявления угроз и нарушений. Она запускается периодически и выполняет тестовую процедуру, которая проверяет все узлы системы безопасности, протокол обмена ключами и ЦРК. При выявлении угрозы неавторизованного доступа к ресурсам системы, обнаружении нарушения прав и полномочий пользователей предупреждается администратор СОБ, и управление передается в ОС.

ОС получает управление при выявлении нарушения любого вида. Функция ОС заключается в прекращении работы системы, восстановлении системы после нарушения в случае нанесения ей ущерба, устранении ущерба, очистки памяти от "мусора". После выявления уязвимых мест системы управление передается в РРС.

РРС, получая управление в человеко-машинном режиме под управлением администратора СОБ, начинает изменять конфигурацию системы безопасности. РРС может исключать любой отказавший работать модуль или поменять на другой, добавить новый и т.д.

Функциональные модули СОБ

Безопасность ресурсов в компьютерных сетях обеспечивается выполнением общепринятых процедур и средств защиты, которые являются составной частью СОБ [4-6]. Ниже рассматриваются эти модули (рис.1).

Модуль управления доступом **–** выполняет функции такие, как идентификация пользователя, регистрация обращений к системе, выдача

немедленных сообщений о нарушениях ответственному оператору - "доверенному терминалу", ограничение доступа к ресурсам и операционной системе, установление подлинности пользователя и сети. Он обеспечивает безопасность информации, ограждая ее от НСД, неавторизованного использования программных продуктов и прав других пользователей.

Посредством процедуры идентификации, каждому пользователю, терминалу, ресурсам, файлам, программам или другим объектам присваивается конкретный уникальный идентификатор, которому, по возможности, сопоставляются контрольные числа, пароль или другие средства контроля с целью минимизации шансов ошибочной идентификации. Использование идентификатора и пароля необходимо не только для опознавания, но и для учета обращений.

Процедура регистрации обращений к системе может помочь определять очаг или причину утечки. Если в системе требуется определенная степень безопасности, то использование идентификации без дополнительных процедур установления подлинности недопустимо.

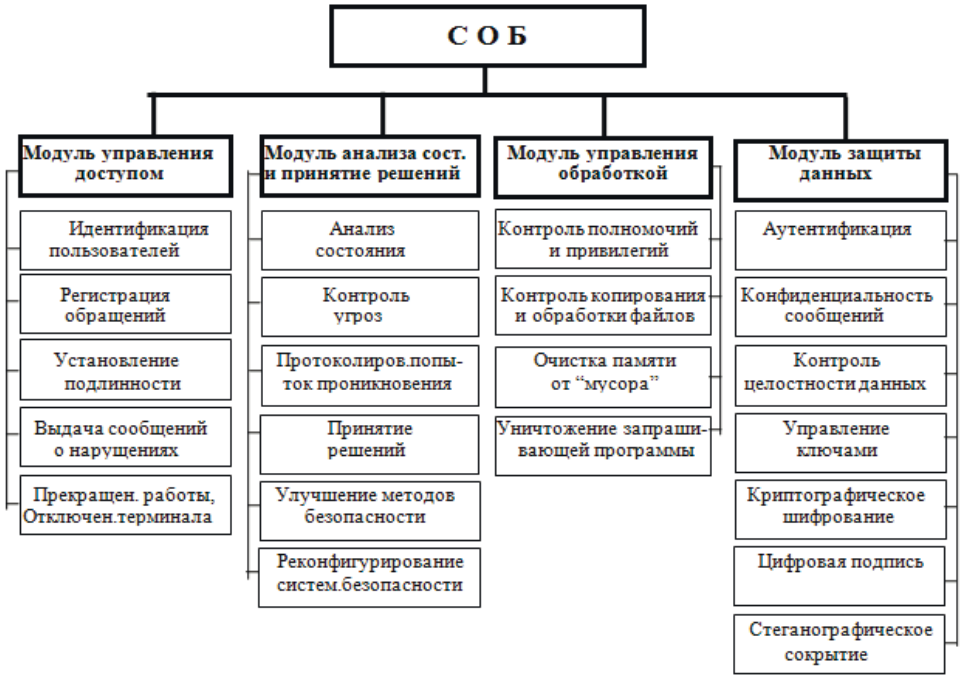

Рис.1. Функциональные модули СОБ

Система идентификации служит базой для процедуры установления подлинности. Установление подлинности заключается в том, чтобы выявить является ли объект тем, за кого себя выдает. Может быть затребована информация различного характера, прежде чем подлинность будет признана установленной. В случаях необходимости обеспечения высокой

степени безопасности может потребоваться периодическая перепроверка в определенных условиях. Для установления подлинности пользователей используются пароли и другие диалоговые методы.

Систему пароля можно использовать и для установления пользователем подлинности сети, когда он желает взаимодействовать с данной системой.

При попытке проникновения в систему или нарушения прав доступа выдается сообщение об этом инциденте на терминал ответственного оператора или "доверенному терминалу" и владельцу информации. Процедура модуля управления доступом показана на рис.2.

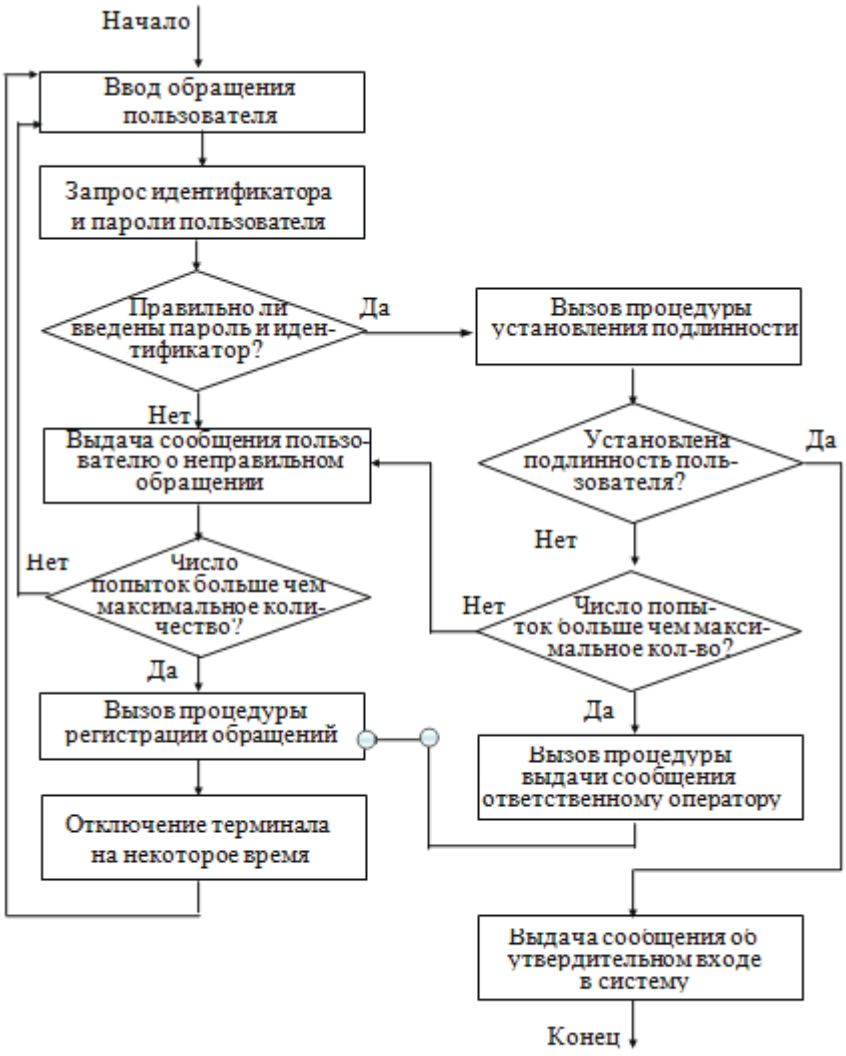

Рис.2. Процедуры модуля управления доступом

Модуль управления обработкой информации. Если методы ограничения доступа не останавливают нарушителя, то он, проникая в систему, может извлечь, изменить или уничтожить информацию в файлах. Процедура контроля обработки позволяет ввести ограничения на обработку файлов, содержащих важную информацию. Файлы на запоминающем устройстве имеют ограничения на чтение, изменение, выполнение. Так, например, какие-то пользователи могут иметь разрешение на чтение, но не иметь разрешения на изменение.

Аналогичным образом можно ввести ограничения на использование любого информационного ресурса (файла, каталога, диска, программы, базы данных и т.д.). Рассмотрим процедуру управления полномочиями и привилегиями, которая содержит двухмерную матрицу категорий доступа $A=\{a_{ij}\}$, $i=\overline{1,n}$ и $j=\overline{1,m}$. Строки матрицы указывают на абонентов, а столбцы на ресурсы сети. Пересечение строки i и столбца j определяет категорию доступа i-го абонента j-му ресурсу. На основе этой матрицы определяется привилегия пользователей, которая может быть изменена с разрешения администратора сети и владельца ресурса.

При неавторизованном запросе файлов, имеющих высокую степень секретности, срабатывает процедура уничтожения запрашивающей программы, которая ее уничтожает, разрывает связь и переходит в состояние "зависания". После завершения выполнения программы, обрабатывающей секретную информацию, которая запрошена законным (авторизованным) пользователем, данные остаются в оперативной памяти, на диске, на ленте и т.д. и злоумышленник может использовать их для своей цели. Поэтому в СОБ включена процедура очистки памяти от остатка и "мусора".

Модуль защиты данных. Когда нарушитель обходит ограничения доступа и контроля обработки, он имеет НСД к данным. В этом случае самый надежный способ предотвращения НСД к данным - это использование криптосистем и применение протоколов безопасности. Имеющийся в СОБ модуль криптографической защиты данных включает в себя процедуры аутентификации, контроля целостности данных, обеспечения секретности обращения и криптографических преобразований для закрытия открытой информации, управления ключами.

Процедура аутентификации выполняет функции установления подлинности информации, пользователя и сети. Аутентификация является жизненно важным вопросом для всех абонентов как коммерческих, так и секретных систем связи. Установление подлинности пользователя означает, что отправитель информации должен заверять свою подпись, т.е. подтвердить, что информация была послана именно тем пользователем, кем была идентифицирована. Установление подлинности сети - это проблема обратная предыдущей, т.е. пользователь определяет, что он имеет

дело с той сетью, которая его интересует. Злоумышленник может выдать себя за пользователя, от чьего имени формирует сообщение, так и за сеть, и, получив информацию, использует ее в своих целях. Получатель требует утверждения подлинности полученной информации, так как она могла быть изменена при передаче по каналу связи.

Процедура контроля целостности управляет средствами обеспечения целостности данных. Эта процедура определяет идентичность информации исходного вида и включает методы обеспечения целостности данных при передаче или хранении информации на носителях.

Криптографические методы шифрования используются для сокрытия смысла открытой информации и обеспечения надежной безопасности от НСД. Злоумышленник, имеющий доступ к данным, должен приложить немало усилий для раскрытия исходного варианта, а это иногда практически невозможно. В настоящее время существует много криптографических систем с большой стойкостью. Среди них особое место занимают Data Encrytion Standart (DES) и криптоалгоритм RSA.

Известно, что для аутентификации и криптографического преобразования используются ключи. Проблема распределения или передачи ключей - одна из главных проблем в системе безопасности. Организация ЦРК или применение протоколов обмена ключами выполняется процедурой управления ключами.

Модуль контроля угроз, анализа состояний и принятия решений занимает основное место в СОБ. Контроль угроз применяется для обнаружения фактов нарушений, попыток проникновения в систему или НСД к данным и обеспечения своевременной реакции на эти факты. Контроль угроз должен включать фиксацию всех исключенных попыток проникновения в систему или к данным, использование неавторизованных процедур, одним словом, любое нарушение политики безопасности.

Любое действие в КС меняет ее состояние. Поэтому состояние КС всегда держится под контролем, выявляются слабости в конфигурации и определяются уязвимые места в средствах защиты. Для анализа состояния протоколируются попытки нарушения, и ведется экспертный анализ. По необходимости принимаются решения о дальнейших действиях: изменение методов защиты или изменение конфигурации КС.

Так как система защиты данных является сложной распределенной системой, то управлять ею можно с помощью методов и средств искусственного интеллекта. При функционировании средств защиты данных можно выделить быстропротекающие процессы (образование и рассасывание очередей в служебных базах данных при проверке привилегий доступа к ресурсам системы), медленные процессы (изменение интенсивности потока запросов на реализацию защитных функций), а также очень

медленные процессы (старение ключей и паролей), отслеживание и анализ протекания которых являются функциями экспертной системы. Структура системы принятия решений по управлению средствами обеспечения безопасности данных содержит функциональные компоненты, которые позволяют автоматизировать и ускорить реакцию при выявлении нарушений в системе.

Подсистема функционального контроля СОБ формирует и посылает в КС тестовые команды для проверки правильности работы средств защиты. Результаты проверок собираются этой же подсистемой в реальном масштабе времени, что обеспечивает возможность оперативного реагирования на возникшие нарушения. Данные о результатах контроля, поступающие из КС, используются для обновления знаний о текущем состоянии КС защиты и в совокупности с предыдущими знаниями служат основой для выработки необходимых управляющих воздействий. Преобразование поступающей информации в форму представления в базе знаний (БЗ) и формирование исходных данных для моделирования работы системы защиты, выполняются подсистемой интерпретации результатов.

Блок логического вывода предназначен для определения типа управляющего воздействия, элементов КС и средств защиты, с помощью которых можно предотвратить или компенсировать возникающие нарушения в сети. При выявлении ситуаций нарушения, которые могут привести к утечке, потере или подмене информации в сети, для обнаружения и локализации места попыток НСД или определения канала утечки информации может использоваться теория нечетких множеств. Для выполнения функций процедуры принятия решений на основе теории нечетких множеств и искусственного интеллекта используется экспертная система (ЭС), которая постоянно контролирует состояние СОБ, дополняет БЗ полученными новыми данными в результате проверок в реальном масштабе времени и делает логический вывод. При обнаружении нарушения прав доступа или полномочий, при определении слабых мест в системе, уязвимости методов шифрования или протокола обмена информацией и в других подобных случаях выдаются управляющие команды и сообщения ответственному оператору. Эти команды могут быть такими, как: немедленно прекратить сеанс, отключить отказавший узел системы, заменить средства защиты, протоколы общения и ключи абонентов и т.д. Таким образом, ЭС может улучшать качество функционирования СОБ в ходе работы. Имеющийся блок самоадаптации по результатам логического вывода меняет параметры системы, чтобы увеличить надежность и обеспечить модульность СОБ. Под модульностью здесь понимается недопустимость утечки информации в случае отказа какого-либо элемента системы.

В процессе управления обеспечением безопасности оператору посылаются сообщения с помощью блока объяснений и диалогового процессора. Ответственный оператор имеет право вмешиваться в процесс управления на любом этапе и ввести управляющие директивы. Все действия оператора должны регистрироваться в БЗ и могут анализироваться с помощью ЭС.

Заключение

Таким образом, в работе рассматриваются проблемы системы обеспечения безопасности для компьютерных сетей. Предложена функциональная структура системы обеспечения безопасности. Приведены основные функции, изложены принципы и порядки действия системы обеспечения безопасности. Более подробно описаны основные функциональные модули системы обеспечения безопасности.

ЛИТЕРАТУРА

1. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие.// Санкт-Петербург. СПб ГУ ИТМО, 2004, 161 с.
2. Ярочкин В.И. Информационная безопасность. М.: Трикста, 2005, 544 с.
3. Аббасов А.М., Алгулиев Р.М., Касумов В.А. Проблемы информационной безопасности в компьютерных сетях. Монография. Баку: Элм, 1998, 235 с.
4. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı. MTN-in nəşriyyat-poliqrafiya mərkəzi. 2009, 340 s.
5. Касумов В.А., Мамедов С.З. Разработка эффективной структуры системы безопасности информации для корпоративных компьютерных сетей. // Наукові праці Одеська національна академія зв'язку ім. О.С.Попова, 2007, № 2. стр.70-73.
6. Gasimov V.A., Amashov Y.A., Aliyeva F.P., Mustafayeva E.A., Mutin D.I. Bolnokin V.E. Development of the information security system effective structure for the distributed computer networks. // IOP Conf. Series: Materials Science and Engineering. Vol. 537, IOP Publishing. 2019. https://iopscience.iop.org/article/10.1088/1757-899X/537/5/052034/pdf.

KOMPÜTER ŞƏBƏKƏLƏRİ ÜÇÜN TƏHLÜKƏSİZLİYİN TƏMİN EDİLMƏSİ SİSTEMİNİN FUNKSİONAL STRUKTURU

F.P.ƏLİYEVA

XÜLASƏ

Məqalədə təhlükəsizliyin təmin edilməsi sisteminin funksional strukturu təklif olunmuşdur. Həmçinin təhlükəsizliyin təmin edilməsi sisteminin əsas funksiyaları, prinsipləri və yerinə yetirilmə ardıcıllıqları verilmiş, əsas funksional modulları təsvir olunmuşdur.

Açar sözlər: təhlükəsizlik sistemi, təhlükəsizliyin təmin edilməsi sistemi, təhlükəsizlik sisteminin funksiyaları, təhlükəsizlik sisteminin modulları

FUNCTIONAL STRUCTURE OF A SECURITY SYSTEM FOR COMPUTER NETWORKS

F.P.ALIYEVA

SUMMARY

The article offers a functional structure of the security system. Also provides the main functions, principles and procedures of action, describes the main functional modules of the security system.

Keywords. security system, security assurance system, security system functions, security system modules