Свердлик. Оптимальные дискретные сигналы. М. "Сов. Радио", 1975 г.

УДК 638.235.231

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Иван Горбач, Маргарита Дума, Виктор Куценко

Государственное предприятие «Укркосмос», г. Киев

Анотація: **Пропонується модель архітектури комплексної системи захисту інформації телекомунікаційної мережі і схема доступу користувачів до інформаційних ресурсів цільових серверів відомчих автоматизованих систем.**

Summary: **Offers a formal architecture model of complex information defense system of telecommunication network and users access scheme to information resources of having a special purpose servers of departmental automated systems.**

Ключові слова: **Сервер, мережа, доступ, пароль, архітектура.**

I Введение

В настоящее время, в связи с ускоренными темпами создания и развития распределенных автоматизированных систем (АС) государственных и банковских структур все более остро встают вопросы защиты информации как по первому или второму уровню защищенности, так и по третьему уровню защищенности. В связи с этим, важным этапом в создании таких систем является этап сертификации и аттестации, что требует с особой ответственностью и тщательностью подходить к вопросу разработки политики безопасности информации как предприятия –владельца, так и самой АС, а также к вопросу разработки комплексной системы защиты информации (КСЗИ), выбора средств защиты.

В настоящем сообщении представлены концептуальные предложения по построению КСЗИ распределенной автоматизированной системы с уровнем защищенности вплоть до третьего уровня.

Под распределенной автоматизированной системой понимается, в данном случае, организационно-техническая система [1], реализующая информационную технологию, объединяющая распределенные по регионам государства (или его части) вычислительные системы (ВС), в том числе, целевые сервера (центра и периферии), транспортную телекоммуникационную систему, персонал и обрабатываемую информацию.

Под защитой от несанкционированного доступа (НСД) будем понимать систему мер, направленную на обеспечение соблюдения правил разграничения доступа (ПРД).

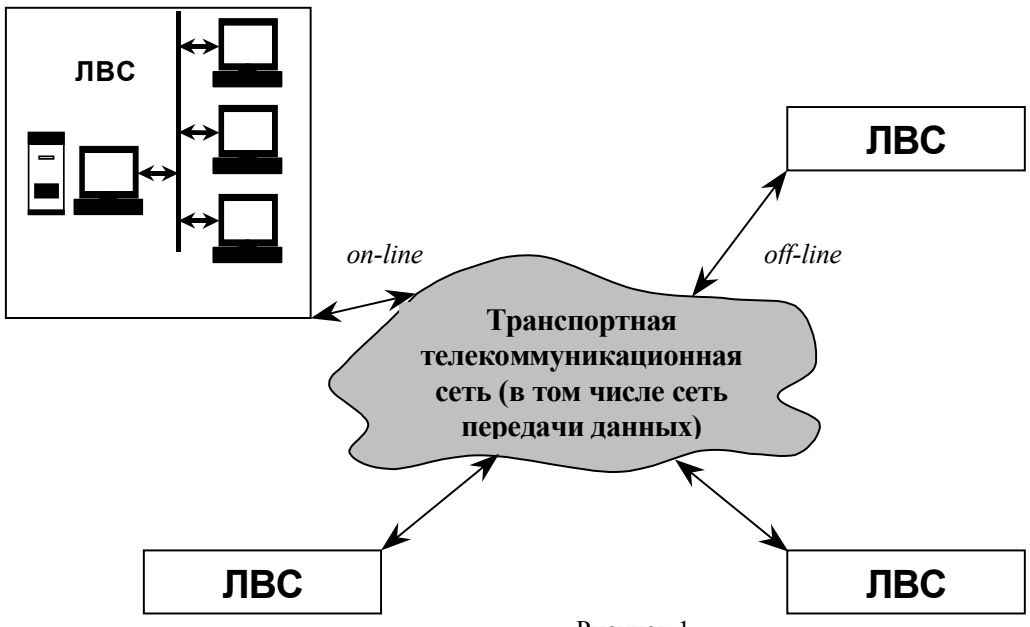

Рисунок 1

II Основная часть

Распределенная автоматизированная система какого-либо ведомства (рисунок 1), как правило, состоит из некоторого количества локальных вычислительных сетей, размещенных по различным регионам страны и взаимодействующих друг с другом по каналам передачи данных транспортной телекоммуникационной сети в режиме удаленного доступа к базам данных (on-line) или в режиме обмена файлами по электронной почте (off-line).

Защита информации от НСД, в данном случае, композиционно разделяется на выполнение следующих задач:

1. Осуществление мероприятий по выполнению ПРД во всех локальных вычислительных сетях (ЛВС) ведомства, реализация технологий защиты информационных ресурсов средствами, позволяющими осуществить полную аттестацию системы уполномоченными органами.
2. Осуществление мероприятий по защите информации в линиях связи между ЛВС ведомства и транспортной телекоммуникационной сетью, если данная ЛВС не включена в зону ответственности КСЗИ транспортной телекоммуникационной сети.
3. Создание многоуровневой системы защиты информации транспортной телекоммуникационной сети по технологии и средствами, позволяющими осуществить аттестацию уполномоченными органами.

По обеспечению первой задачи возможна реализация программного комплекса защиты информационных ресурсов на базе технологии сервера безопасности, причем, заимствованный программный продукт, в нашем случае, не дает возможности аттестации системы и непрерывной модификации этого программного комплекса.

Концептуальную основу создания данного программного продукта, обеспечивающего требуемую степень защиты информационных ресурсов, составляют положения:

- по сети не должна быть передана парольная информация;
- разрешение на доступ к обслуживанию в сети не может быть послано пользователю в виде обычного сообщения, а применяется шифрование современными криптографическими методами.

Доступ пользователей к сетевым серверам, файлам, приложениям, принтерам осуществляется по следующей схеме. Работа начинается с регистрации пользователя в идентификационном сервере. Идентификационный сервер, обладая базой данных обо всех пользователях, определяет его пароль, выдает «разрешение на получение разрешения» (ticket-granting ticket) и специальный код сеанса, решая проблему защиты пароля пользователя.

На следующем этапе пользователь со своей рабочей станции взаимодействует с сервером выдачи разрешений на получение доступа к требуемым ресурсам сети. Запрос к данному серверу содержит: имя пользователя, сетевой адрес пользователя, отметку времени, код сеанса, время жизни разрешения идентификационного сервера и собственно «разрешение на получение разрешения», а также, аутентикатор (authenticator). Все взаимодействие осуществляется с неоднократным шифрованием различными кодами.

Поскольку аутентикатор используется для идентификации пользователя всего один раз и только в течение определенного периода времени, становится практически невозможным одновременный перехват и «разрешения на получение разрешения» и аутентикатора для последующих попыток несанкционированного доступа к ресурсам сети.

После успешной идентификации пользователя сервер выдачи разрешений отсылает пользователю разрешение на доступ к ресурсам сети и новый код сеанса в зашифрованном виде. Следующее за этим обращение к целевому серверу, ресурсы которого нужны пользователю, шифруются с помощью нового кода сеанса.

Для обеспечения еще более высокого уровня защиты осуществляется идентификация целевого сервера, который, выделив код сеанса, расшифровывает аутентикатор, прибавляет к отметке времени единицу, зашифровывает полученную информацию с помощью кода сеанса и отсылает пользователю. Расшифровка этого сообщения позволяет пользователю идентифицировать целевой сервер. Использование в качестве кода отметки времени дает уверенность в том, что пришедший ответ от целевого сервера не является повтором ответа на какой-либо предыдущий запрос.

Реализация настоящей технологии совместно с выполнением других мероприятий позволяет обеспечить выполнение, как первой, так и в существенной мере, второй задачи.

Осуществление мероприятий по решению третьей задачи, связанной с созданием системы защиты информации транспортной телекоммуникационной сети, требует разработки нового подхода к организации защиты информации, который бы обеспечивал реализацию следующих аспектов защиты:

- реализацию в пределах одной системы различных уровней защищенности для различных объектов защиты;
- реализацию в пределах одной системы различных функциональных профилей защищенности объектов;
- динамическую адаптацию комплексной системы защиты информации в зависимости от изменяющейся модели угроз;

- аттестацию всей системы в целом уполномоченными органами.

Сформулированные аспекты защиты обуславливают необходимость разработки соответствующей архитектуры системы защиты информации. Главной целью, при этом, является создание модели архитектуры, инвариантной относительно аппаратно-программных средств АС.

Отправной точкой для создания подобной модели архитектуры является семиуровневая модель архитектуры взаимодействия открытых систем (ВОС) международной организации (МОС) ISO 7498.

Обеспечение защиты информации в рамках ISO 7498 регламентируется механизмами и услугами, определенными в документе ISO 7498.2.

Базовая эталонная модель ВОС МОС включает собственно модель, протоколы и услуги сетевого взаимодействия распределенных систем.

Услуги отдельных уровней выполняются специфицированными протоколами, регламентирующими взаимодействия компонентов одноименных уровней. Для согласования архитектуры КСЗИ с архитектурой сети, реализуемой как открытая система взаимодействия распределенных объектов, КСЗИ можно представить в виде трех иерархически взаимосвязанных компонентов: модель КСЗИ сети; услуги по защите информации сети; механизмы защиты информации сети.

Модель КСЗИ сети специфицирует правила и особенности реализации услуг и механизмов по защите информации.

Услуги по защите информации регламентируют функциональные особенности КСЗИ сети, необходимые для реализации требуемого уровня защиты информации.

Механизмы по защите информации включают множества правил, способов и алгоритмов, позволяющих эффективно реализовать требуемые услуги по защите информации.

Таким образом, становится возможной рациональная адаптация архитектуры КСЗИ сети в семиуровневую архитектуру сети.

Для обеспечения унификации архитектурных показателей с целью обеспечения требуемого уровня защиты информационных ресурсов в сети, архитектура КСЗИ сети представляется следующей схемой (см. рисунок 2):

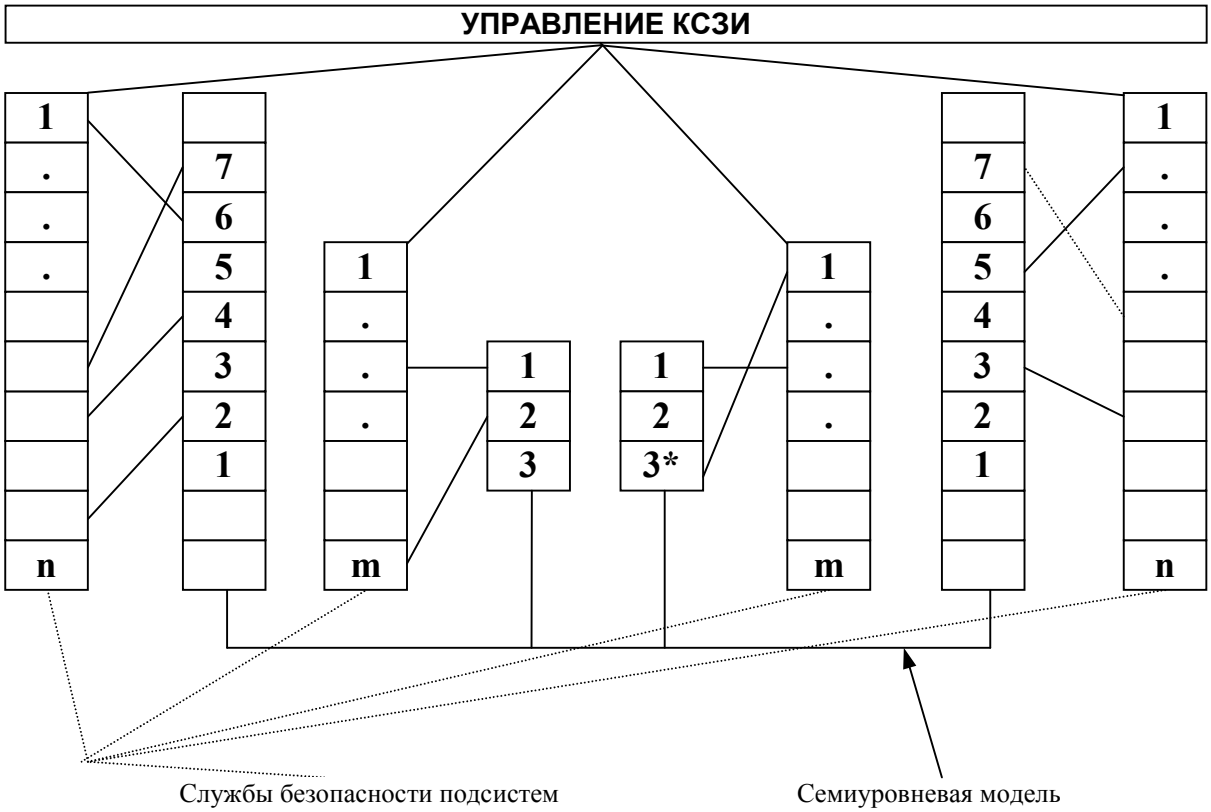

Рисунок 2

Подобная архитектура КСЗИ сети позволяет реализовать распределенную систему управления ресурсами в части защиты информации в сети.

Технология управления ресурсами реализуется на основе информации, полученной от агентов служб безопасности на соответствующих уровнях модели ВОС МОС.

Предлагаемая модель включает следующие компоненты:

- операционная среда управления безопасностью (ОСУБ), которая обеспечивает управление различными по уровню и профилю защищенности службами (услугами) защиты информации;
- службы защиты информации каждой автономной сетевой компоненты, взаимодействующие с агентами (механизмами защиты информации);
- встроенные в межуровневые интерфейсы (точки доступа к услугам) агенты.

При этом реализация конкретных функций по защите информации, номенклатура которых определяется моделью угроз и требуемым функциональным профилем защищенности, может обеспечиваться за счет применения стандартных программно-аппаратных средств –механизмов защиты.

При разработке системы защиты информации обеспечивается идеологическое единство ОСУБ и механизмов защиты (МЗ), а возможность их взаимодействия гарантируется согласованным набором состоятельных протоколов верхних уровней.

Иерархическое построение ОСУБ может включать: главный центр, зональные и местные центры, а также агенты управления безопасностью, осуществляющие непосредственное управление МЗ.

Основной целевой функцией ОСУБ является удержание состояния защищенности объектов системы на заданном уровне.

Предлагаемая архитектура не противоречит требованиям каких-либо международных и отечественных стандартов и рекомендаций. Напротив, она позволяет при необходимости учесть конкретные условия реализации системы защиты информации с требуемыми характеристиками. Инвариантность операционной среды относительно отдельных алгоритмов защиты информации, реализованной в соответствии с предполагаемой архитектурой, позволяет внедрять в систему любые алгоритмы и технологии по защите отдельных участков прохождения информации по сети. Это означает, например, что в случае изменения стандарта шифрования (или предъявления дополнительных требований) оболочка системы управления КСЗИ сети остается неизменной, меняется только соответствующий механизм по защите информации.

Создание системы защиты информации в соответствии с настоящей моделью позволяет:

- обеспечивать требуемый уровень защиты информации на отдельных уровнях архитектуры системы, построенной в соответствии с эталонной моделью взаимодействия открытых систем;
- стратифицировать слои управления безопасностью для отдельных ведомств, реализуя многоуровневость системы защиты информации (одновременная обработка информации с различными требуемыми уровнями и профилями защищенности);
- постоянно совершенствовать МЗ и услуги, не затрагивая структуру управления безопасностью;
- реализовать любую прикладную подсистему защиты информации (в том числе технологию сервера безопасности).

III ВЫВОДЫ

В настоящей работе на основе декомпозиции общей схемы построения распределенной автоматизированной системы приведены концептуальные предложения по обеспечению в ней защиты информации от первого уровня до третьего уровня защищенности.

Приведенная схема доступа пользователей к информационным ресурсам целевых серверов АС показывает возможность надежной защиты баз данных, а представленная формальная модель архитектуры комплексной системы защиты информации транспортной телекоммуникационной сети показывает возможность реализации системы, обеспечивающей фундаментальные свойства: конфиденциальность, целостность, доступность, наблюдаемость.

Эта модель согласуется с семиуровневой моделью ВОС и является инвариантной относительно сетевых протоколов. Синтез угроз информационным ресурсам осуществляется на основе свойств объектов отдельных уровней модели ВОС. Это позволяет создавать прикладные системы с требуемым уровнем защиты информационных ресурсов в распределенных АС ведомств и банковских структур. Изложенные концептуальные предложения позволяют обеспечить положительные результаты аттестации системы в целом.

Литература: Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. - НД ТЗИ 1.1-003-99