УДК 004.75

АЛГОРИТМ РАСПРЕДЕЛЕНИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Дмитрий Анатольевич Таров
к.п.н., доцент
tarov1970@rambler.ru
г. Елец

Елецкий государственный университет им. И.А. Бунина

Аннотация. В статье обосновывается и излагается алгоритм распределения функций безопасности распределенной вычислительной сети. При разработке распределения функций безопасности автор предлагает исходить из соотношения «пропускная способность канала /стоимость аппаратного и программного обеспечения», что придает алгоритму определенную гибкость. Статья содержит покомпонентное описание алгоритма и его подробную блок-схему. Автором предложены рекомендации, целью которых служит повышение пропускной способности канала как в случае низкоскоростного, так и высокоскоростного каналов. В статье рассмотрена работа алгоритма распределения функций безопасности распределенной вычислительной сети на примере корпоративной сети, построенной по принципу распределенной информационно-вычислительной системы на базе технологии локальных вычислительных сетей и организационно представляющей собой несколько функциональных контуров, объединенных в единый комплекс. Комплекс состоит из локальной вычислительной сети главного офиса, локальной вычислительной сети удаленной площадки (в том же населенном пункте) и локальной вычислительной сети удаленного офиса (в другом населенном пункте) Физически связь между офисами осуществляется через Интернет, доступ в который предоставляется различными провайдерами. Связь главного офиса с удаленной площадкой осуществляется через обычный модем по выделенной линии. Статья содержит конкретные рекомендации по аппаратным и программным компонентам защищаемой сети, организации шифрования внутрисетевого трафика, основанные на комплексе руководящих документов по защите от несанкционированного доступа, разработанный Гостехкомиссией при Президенте РФ. Предлагаемая автором конфигурация защищает сеть от несанкционированного стороннего анализа сетевого трафика, подмены одного из участников TCP-соединения, а также от угрозы отказа в обслуживании со стороны внешней сети.

Ключевые слова: распределенная вычислительная сеть, алгоритм распределения функций безопасности, шифрование внутрисетевого трафика.

Рассмотрим алгоритм распределения функций безопасности по компонентам системы. При разработке распределения функций безопасности будем исходить из соотношения *«пропускная способность канала /стоимость аппаратного и программного обеспечения»* [1]. Может сложиться ситуация, когда при заданной стоимости достигнута скорость передачи данных, которая может оказаться ниже максимально возможной.

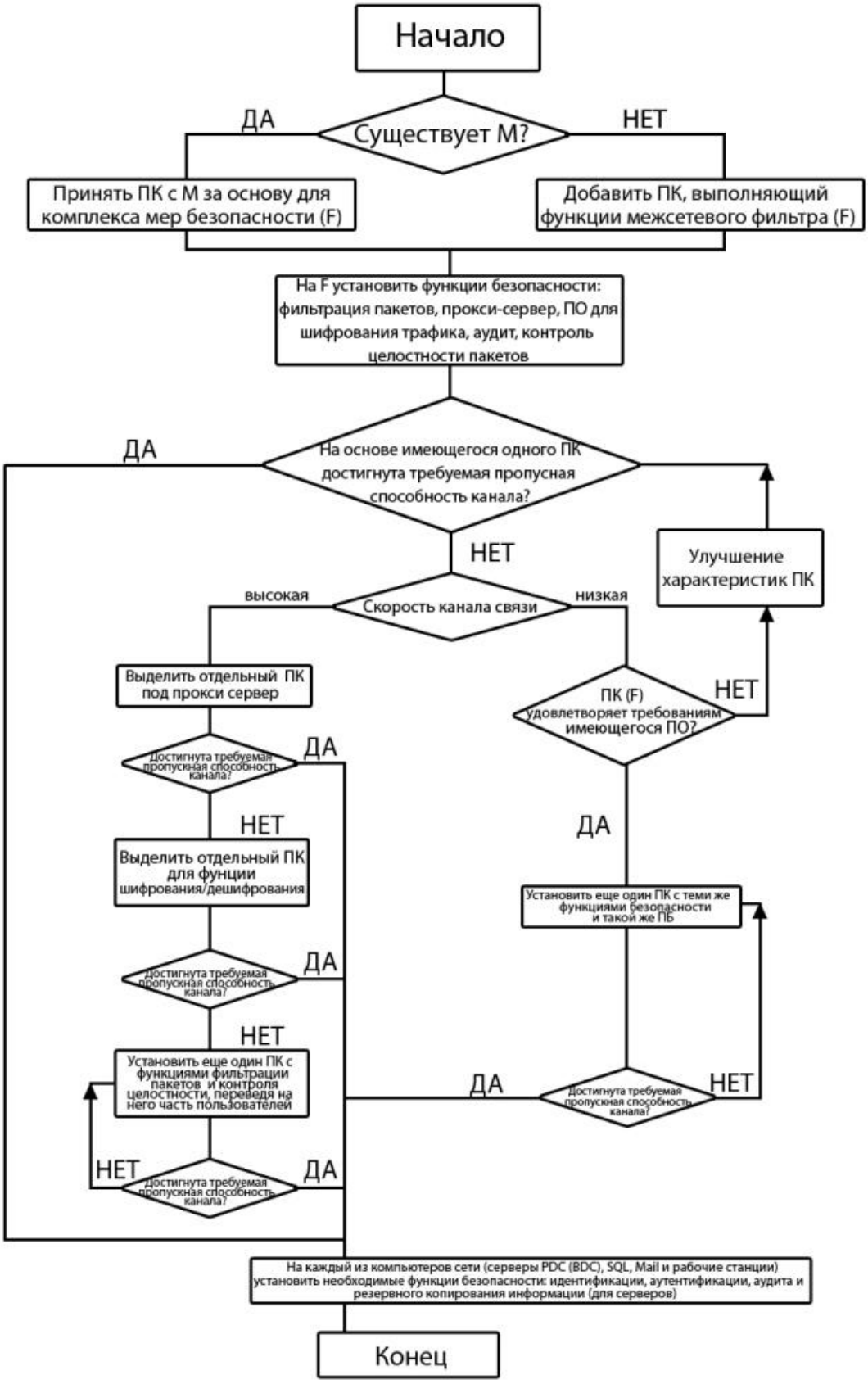

Рис.1. Блок-схема алгоритма распределения функций безопасности распределенной вычислительной сети.

Проектировщик имеет возможность использовать при проектировании архитектуры безопасности распределенной вычислительной сети (АБ РВС) или стоимостные, или скоростные критерии, что придает алгоритму определенную гибкость.

В общем виде предлагаемый алгоритм состоит из следующих практически независимых элементов:

- Построение архитектуры безопасности межсетевых экранов (АБ МЭ) в соответствии с требуемым уровнем защищенности, исходя из соотношения «пропускная способность канала /стоимость аппаратного и программного обеспечения». Обеспечение защитных функций межсетевых экранов.
- Обеспечение надлежащего уровня безопасности на всех имеющихся в РВС котроллерах доменов (PDC).
- Обеспечение безопасности рабочих станций пользователей, в соответствии с требуемым уровнем защиты.
- Обеспечение надлежащего уровня защиты почтовых серверов.
- Организация защиты внутренних WWW- и FTP-серверов, если таковые существуют.

Общая блок-схема такого алгоритма представлена на рис. 1.

Существующий в рассматриваемой системе маршрутизатор можно принять за основу для создаваемого комплекса мер безопасности. Если маршрутизатор отсутствует, то необходимо добавить, по крайней мере, один компьютер, выполняющий функции межсетевого фильтра. После этого, на межсетевой фильтр устанавливаются относящиеся к нему функции безопасности. Если на основе имеющегося компьютера не достигается требуемая пропускная способность канала, то:

- в случае низкоскоростного канала следует рассмотреть возможность ее увеличения путем повышения производительности одного компьютера в соответствии с требованиями установленного программного обеспечения (увеличить мощность процессора, увеличить объем оперативной памяти и т.д.). Если при этом полученная пропускная способность является недостаточной, то необходимо добавить один или несколько компьютеров с тем же набором функций безопасности и такой же политикой безопасности;
- в случае высокоскоростного канала имеет смысл выделить функции прокси-сервера на отдельный компьютер. В случае недостаточного увеличения пропускной способности можно выделить отдельную машину для шифрования/дешифрования трафика. Если вышеперечисленные меры не приносят необходимого результата, то следует добавить один или несколько компьютеров с необходимым набором функций безопасности и такой же политикой безопасности, что приведет к распараллеливанию коммуникационного трафика.

В случае наличия нескольких выходов в незащищенную сеть эти действия необходимо повторить для каждого из имеющихся выходов.

На каждом сервере (контроллере домена) необходимо установить соответствующие функции безопасности:

- идентификация и аутентификация;
- аудит;
- контроль целостности;
- система восстановления после сбоев;
- в случае, если требуется высокий уровень защиты, на каждый сервер необходимо установить средства для шифрования внутрисетевого трафика и, возможно, средства для криптографической защиты информации на дисках.

Изначально предполагается, что система содержит, по крайней мере, один сервер,

и одну рабочую станцию.

На каждой пользовательской рабочей станции необходимо реализовать соответствующие функции безопасности:

- идентификация и аутентификация;
- аудит;
- в случае необходимости высокого уровня защищенности на рабочие станции необходимо установить средства для шифрования сетевого трафика и, в некоторых случаях, средства для криптографической защиты информации на дисках.

На почтовом сервере в зависимости от требуемого уровня защищенности необходимо реализовать следующее:

- идентификация и аутентификация;
- аудит;
- контроль целостности;
- система восстановления после сбоев;
- средства для шифрования данных на дисках.

В зависимости от уровня защищенности на почтовых серверах следует установить почтовые протоколы IMAP или POP, SMTP, при необходимости более высокого уровня защищенности – IMAP через SSL, SMTP через SSL.

На внутренних WWW- и FTP-серверах необходимо установить соответствующие им функции безопасности:

- идентификация и аутентификация;
- аудит;
- контроль целостности;
- система восстановления после сбоев;
- средства для поддержки протокола HTTPS для WWW сервера (SFTP для FTP-сервера);
- средства для криптографической защиты информации на дисках для обеспечения высокого уровня защищенности.

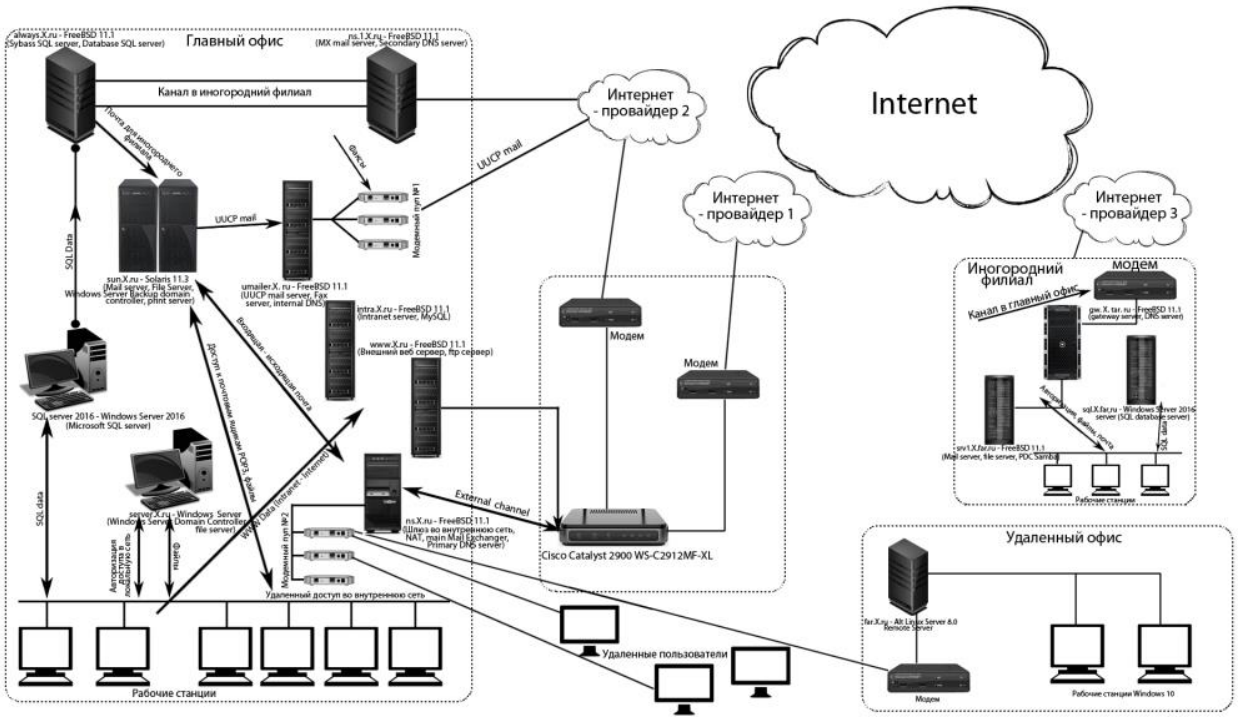

Рис. 2. Пример архитектуры корпоративной сети.

Авторизация прав доступа пользователей происходит в случае обращения к контроллеру домена или почтовому серверу – на соответствующем сервере, в остальных случаях – на контроллере домена.

В качестве примера работы алгоритма рассмотрим РВС некоторой компании, архитектура которой показана на рис. 2.

Корпоративная сеть рассматриваемой компании построена по принципу распределенной информационно-вычислительной системы на базе технологии локальных вычислительных сетей (ЛВС). Организационно сеть представляет собой несколько функциональных контуров, объединенных в единый комплекс. Имеется ЛВС главного офиса, ЛВС удаленной площадки (в том же населенном пункте) и ЛВС удаленного офиса (в другом населенном пункте). Физически связь между офисами осуществляется через Интернет. Доступ в Интернет предоставляется различными провайдерами. Связь главного офиса с удаленной площадкой осуществляется через обычный модем по выделенной линии.

Перечень серверов, рабочих мест и устанавливаемое на них системное ПО приведены в табл. 1.

Таблица 1.

Функциональное назначение	**Системное ПО**	**Кол-во**
SQL Server 2016 – сервер БД	Windows Server 2016, SQL server 2016	1
Sun – mail, BDC, file, print	Solaris 11.3	1
Server – PDC, file, print	Windows Server 2016	1
umailer – UUCP mail, DNS	FreeBSD 11.1	1
Телекоммуникационный сервер nsl.X.ru	FreeBSD 11.1	1
Телекоммуникационный сервер ns.X.ru	FreeBSD 11.1	1
Внутренний WWW-сервер intra.X.ru	FreeBSD 11.1, Apache 2.4, MySQL	1
Внешний WWW-сервер www.X.ru	FreeBSD 11.1, Apache 2.4	1
Телекоммуникационный сервер always.X.ru	FreeBSD 11.1, SyBase IQ, SQL server 2016	1
SRVl-BDC, mail	FreeBSD 11.1, Samba 4.7.5	1
sql.X.far.ru – сервер БД	FreeBSD 11.1	1
Телекоммуникационный сервер gw.X.far.ru	FreeBSD 11.1	1
Телекоммуникационный сервер far.X.ru	Alt Linux Server 8.0	1
Рабочие места главного офиса	Windows 10	12
Рабочие места удаленного офиса	Windows 10	67

В состав сетевого оборудования входят:

- адаптеры для подключения рабочих мест, локальных серверов и серверов к ЛВС;
- коммутаторы для организации взаимодействия между отдельными сегментами ЛВС;
- маршрутизаторы для организации взаимодействия ЛВС с глобальной сетью Интернет.

В качестве основного сетеобразующего оборудования ЛВС главного офиса используется коммутирующий концентратор Cisco Catalyst 2900 WS-C2912MF-XL, имеющий 12 коммутируемых портов Ethernet 100Base-TX. В коммутаторе имеется возможность фильтрации адресов назначения и выбора вариантов коммутации: с промежуточным хранением данных или сквозная.

Для подключения ЛВС к глобальным сетям связи используется маршрутизатор Cisco ISR4321/K9, вынесенный во внешний сегмент этой локальной сети и обеспечивающий подключение по синхронным каналам к двум независимым интернет-провайдерам с помощью модемов для оптоволоконных линий. Управление маршрутизатором осуществляется через порт консоли или по сети по протоколу SNMP.

В качестве исходной точки для разработки системы защиты ресурсов РВС от несанкционированного доступа (НСД) был использован комплекс руководящих документов по НСД, разработанный Гостехкомиссией при Президенте РФ.

На телекоммуникационные сервера nsl.X.ru, ns.X.ru, gw.X.far.ru, а также на внешний WWW-сервер www.X.ru установлен межсетевые экраны (скомпилировано ядро FreeBSD соответствующим образом – с поддержкой IPFW).

Поток данных между главным офисом и филиалом подвергнут шифрованию. Для этого создан шифрованный канал между телекоммуникационными серверами Always и gw.X.far.ru с использованием алгоритма шифрования Triple DES.

В целях защиты внутренних информационных потоков, а также безопасного удаленного администрирования, на всех серверах под управлением ОС FreeBSD следует установить демон SSHD, обеспечивающий шифрование трафика и отключить демон telnetd. Также на всех серверах под управлением Windows Server 2016 установить программное обеспечение, обеспечивающее шифрование трафика. На сервере SRV1 установлено программное обеспечение, поддерживающее IPsec. На всех серверах и рабочих станциях должен вестись журнал аудита.

Доступ к внутреннему WWW-серверу Intra должен осуществляться по протоколу HTTPS. Доступ к FTP-серверу должен происходить по протоколу SFTP. Чтение почты должно осуществляться по протоколу IMAP4 через SSL или POP3 через SSL.

Предложенная конфигурация защищает сеть от несанкционированного стороннего анализа сетевого трафика, подмены одного из участников TCP-соединения, а также от угрозы отказа в обслуживании со стороны внешней сети.

Список литературы

1. Просихин В.П., Чураев Л.А. Построение алгоритма проектирования архитектуры безопасности распределенных вычислительных систем // Проблемы информационной безопасности высшей школы, МИФИ, 2000, тезисы докладов, с. 126-127.

ALGORITHM OF DISTRIBUTION OF SAFETY FUNCTIONS OF A DISTRIBUTED COMPUTER NETWORK

D.A. Tarov
Cand. Sci. (Pedagogy), associate professor
tarov1970@rambler.ru
Yelets

Bunin Yelets State University

Abstract. The article justifies and outlines the algorithm for distributing the security functions of a distributed computer network. In developing the distribution of safety functions, the author suggests starting from the ratio "channel capacity / cost of hardware and software", which gives the algorithm some flexibility. The article contains an exploded description of the algorithm and its detailed block diagram. The author proposes recommendations aimed at improving the channel capacity of the channel in both low-speed and high-speed channels. The article considers the work of the algorithm for distributing the security functions of a distributed computer network using the example of a corporate network built on the principle of a distributed information and computing system based on the technology of local computer networks and organizationally representing several functional circuits that are integrated into a single complex. The complex consists of a local area network of the main office, a local computer network of a remote site (in the same locality) and a local computer network of a remote office (in another locality). Physical communication between offices is via the Internet, access to which is provided by various providers. The main office is connected to the remote site via an ordinary modem on a dedicated line. The article contains specific recommendations on the hardware and software components of the protected network, the organization of encryption of intranetwork traffic, based on a set of guiding documents for protection against unauthorized access, developed by the State Telecommunications Commission under the President of the Russian Federation. The configuration offered by the author protects the network from unauthorized third-party analysis of network traffic, the substitution of one of the participants of the TCP connection, as well as the threat of denial of service from the external network.

Keywords: distributed computer network, algorithm for distribution of security functions, encryption of intranetwork traffic.

References

1. Prosihin, V.P., Churaev, L.A. (2000) Postroenie algoritma proektirovaniia arhitektury` bezopasnosti raspredelenny`kh vy`chislitel`ny`kh sistem [Postroenie algoritma proektirovanija arhitektury bezopasnosti raspredelennyh vychislitel'nyh system]. // Konferencija "Problemy infor-macionnoj bezopasnosti vysshej shkoly", MIFI, tezisy dokladov, s. 126-127.