

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Специализация -

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

СИСТЕМА ЗАЩИТЫ И КОНТРОЛЯ СЕТЕВОГО ТРАФИКА

Студент



Моисеев Андрей Юрьевич

Руководитель начальник НИС-1022 АО «ПНИЭИ»



Романов И.О.

Нормоконтролёр



Иванов А.П.

Рецензент начальник НИС-102 АО «ПНИЭИ»



Оськин Р.С.

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой



С.Л. Зефилов

Работа защищена с отметкой хорошо (протокол заседания ГЭК
от 25.06.20 № 13)

Секретарь ГЭК



А.П. Иванов

Пенза 2020

Содержание

Введение.....	6
1 Анализ проблемы защиты информации, обрабатываемой с использованием сетевых технологий.....	8
1.1 Проблематика и основные направления защиты информации	8
1.2 Сеть как объект защиты информации.....	10
2 Обзор существующих механизмов защиты, применяемых в IP-сетях	15
2.1 Общие сведения.....	15
2.2 Предпусковой контроль.....	16
2.3 Аутентификация субъектов доступа	17
2.4 Разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям	17
2.5 Регистрация и оперативное оповещение о событиях, происходящих в системе и имеющих отношение к безопасности.....	18
2.6 Криптографическое закрытие хранимых и передаваемых по каналам связи данных	19
2.7 Контроль целостности сетевых пакетов	21
2.8 Изоляция (защита периметра) компьютерных сетей (скрытие внутренней структуры и адресации путем трансляции адресов).....	22
2.9 Контроль целостности программного обеспечения	23
2.10 Механизм защиты от несанкционированного доступа	24
2.11 Обнаружение и противодействие атакам (опасным действиям нарушителей)	26
3 Разработка архитектуры системы связи организации с учетом системы защиты и контроля сетевого трафика	29
3.1 Место СЗИКСТ в системе связи организации	29
3.2 Криптографическая защита комплекса.....	30
4 Разработка и описание алгоритмов работы механизмов защиты информации, реализуемых в подсистеме защиты сетевого трафика	35

4.1	Механизм аутентификации	36
4.2	Механизм предпускового контроля	38
4.3	Регистрация и оперативное оповещение о событиях, происходящих в системе и имеющих отношение к безопасности.....	43
4.4	Механизм контроля целостности программного обеспечения	43
4.5	Механизм защиты от несанкционированного доступа к внутренним элементам маршрутизатора.....	46
4.6	Механизм контроля целостности ключевой информации.....	46
4.7	Алгоритм функционирования контрольно-блокировочных механизмов защиты системы защиты и контроля сетевого трафика	49
4.8	Обоснование отказа от механизмов защиты	51
5	Разработка и описание алгоритмов работы, механизмов фильтрации пакетов информации, реализуемых в подсистеме контроля сетевого трафика.....	53
5.1	Механизм межсетевого экранирования	53
6	Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	59
6.1	Общие сведения.....	59
6.2	Статическая нагрузка.....	59
6.3	Постоянная концентрация внимания	60
6.4	Большой объем информации, обрабатываемый в единицу времени	60
6.5	Повышенный уровень электромагнитного излучения	60
	Заключение	63
	Список используемых источников.....	65

Сокращения

В работе применяются следующие сокращения:

- АЛУ - арифметико-логическое устройство;
- АЦП - аналогово-цифровой преобразователь;
- Гбит/с - гигабит в секунду;
- ЗИ - защита информации;
- ИБ - информационная безопасность;
- ИС - информационная система;
- КДСЧ - ключ датчика случайных чисел;
- КИ - ключевая информация;
- МДСЧ - маска датчика случайных чисел;
- НСД - несанкционированный доступ;
- ОЗУ - оперативно запоминающее устройство;
- ОС - операционная система;
- ПДСЧ - программный датчик случайных чисел;
- ПЗУ - постоянно запоминающее устройство;
- ПК - персональный компьютер;
- ПО - программное обеспечение;
- ПЭВМ - персональная электронно-вычислительная машина;
- РД - руководящие документы;
- СЗИКС - система защиты и контроля сетевого трафика;
- СКЗИ - средство криптографической защиты;
- СОВ - система обнаружения вторжений;
- СП - случайная последовательность;
- Тбит/с - терабит в секунду;
- ЭЦП - электронно-цифровая подпись;
- ARP - Address Resolution Protocol;
- DHCP - Dynamic Host Configuration Protocol;

- DNS - Domain Name System;
- ESP - Encapsulating Security Payload;
- FTP - File Transfer Protocol;
- HTTP - Hypertext Transfer Protocol;
- HTTPS - Hypertext Transfer Protocol Secure;
- IMAP - Internet Message Access Protocol;
- IPX - Internetwork Packet Exchange;
- IRC - Internet Relay Chat;
- LAN - Local Area Network;
- MITM - Man-In-The-Middle Attack;
- NNTP - Network News Transfer Protocol;
- NTP - Network Time Protocol;
- POP3 - Post Office Protocol 3;
- POPS - Protocol On Persistent Organic Pollutants;
- QOTD - Quote Of The Day;
- RFC - Request For Comments;
- RIP - Routing Information Protocol;
- RTSP - Real Time Streaming Protocol;
- SMTP - Simple Mail Transfer Protocol;
- SNMP - Simple Network Management Protocol;
- SSH - Secure Shell;
- UDP - User Datagram Protocol;
- USB - Universal Serial Bus;
- VPN - Virtual Private Network;
- WAN - Wide Area Network;
- WWW - World Wide Web;
- XDMCP - X Display Manager Control Protocol.

Введение

С момента установления первого сетевого соединения между двумя компьютерами одной сети и до наших дней прошло чуть более 50 лет. За это время сетевые технологии претерпели множество изменений. Одним из таких изменений является качественный скачок пропускной способности сети, если на первых этапах развития сетевых технологий считалось невозможным реализовать канал связи со скоростью 1 Гбит/с, то на сегодняшний день существуют оптоволоконные кабели, позволяющие достигать скорости 255 Тбит/с. Появились сотни различных сетевых протоколов, технологии виртуальных частных сетей, IP-телефония, беспроводные сети и др., помимо этого постоянно модернизируется аппаратная составляющая, разрабатываются новые схемотехнические решения. Сетевые технологии развиваются настолько быстро потому, что в современном мире информация является основным активом большинства организаций. Для фондовых рынков, например, важна скорость получения информации о курсе облигаций, где даже миллисекунда отставания от конкурентов может приводить к потерям миллионов долларов прибыли.

Но даже учитывая необходимость высокоскоростного сетевого взаимодействия, если при передаче информации произошли искажения, изменения это приводит к потере прибыли, а также может иметь ряд последствий для самой организации. Например, злоумышленник может сканировать сеть организации на наличие возможности реализации сетевых атак, либо заведомо зная об уязвимостях портов сетевого оборудования или отсутствии контроля сетевого трафика может использовать их для получения конфиденциальной информации.

Сетевые атаки могут реализовываться как из внешних сетей, так и из внутренних, но ввиду организационных мер защиты, применяемых предприятиями, в большинстве случаев сетевые атаки, реализуются из внешней сети. Для обеспечения конфиденциальности, целостности и доступности

информации необходимо использовать ряд механизмов защиты. Также ввиду необходимости системного применения множества различных механизмов, целесообразно реализовать такую систему защиты в качестве отдельного модуля, который может встраиваться в пограничный маршрутизатор и обеспечивать свойства безопасности информации.

Таким образом, актуальность выпускной квалификационной работы обосновывается актуальностью сетевых компьютерных атак, а также необходимостью защиты конфиденциальной информации организации от несанкционированного доступа.

Для обеспечения безопасности информации, циркулирующей в сети связи организации, необходимо использовать систему защиты и контроля сетевого трафика, функционирующую на пограничном маршрутизаторе корпоративной сети связи. Вариант реализации системы с применением различных механизмов защиты информации представлен в выпускной квалификационной работе.

Целью работы является разработка алгоритмов функционирования механизмов защиты информации, реализуемых в составе системы защиты и контроля сетевого трафика.

Основными задачами выпускной квалификационной работы является рассмотрение существующих механизмов защиты применяемых в IP-сетях, выбор и обоснование необходимости применения данных механизмов, а также разработка алгоритмов функционирования выбранных механизмов защиты в системе защиты и контроля сетевого трафика.

1 Анализ проблемы защиты информации, обрабатываемой с использованием сетевых технологий

1.1 Проблематика и основные направления защиты информации

В современном быстро меняющемся мире эффективность работы с информацией является одним из важнейших факторов успеха. Защита конфиденциальной информации получила особенную актуальность в связи с большим количеством атак как на коммуникативные средства связи, так и на данные, хранимые на различных видах электронных носителей. Количество данных и информации, сохраняемых в цифровой форме, постоянно увеличивается.

Ежедневно в мире создается более миллиарда файлов, которые хранятся на серверах компаний, личных компьютерах работников предприятий, персональных компьютерах других пользователей. По мере роста объемов данных, с которыми оперируют пользователи информационных систем, возрастают трудности успешного ведения бизнеса, повышается вероятность ошибочных действий, уменьшается степень защищённости информационных систем.

Для более удобной работы сотрудников: оперативного обмена, гибкой обработки и хранения информации строятся компьютерные сети. Как следствие, возникает проблема: защита обрабатываемой на средствах вычислительной техники и передаваемой по сети информации.

Защита информации внутри корпоративной сети является одной из основных задач, которые разрешаются при построении информационной безопасности на предприятии. Для её обеспечения необходимо разграничить доступ к информационным ресурсам между сотрудниками и предотвратить как несанкционированный доступ к данным изнутри корпоративной сети, так и извне.

Также необходимо обеспечение свойств безопасности информации, циркулирующей в сети связи организации, а также передаваемой на съемных носителях информации. Так как эти цифровые данные являются результатом работы большинства организаций, то нарушение свойств информации влечет за собой появление ущерба и нарушении бизнес-функций организаций. Обеспечение свойств безопасности информации - это залог успеха предприятия.

В области защиты информации наиболее актуальными являются атаки, направленные на:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение доступности информации;
- нарушение работоспособности информационно-вычислительных систем.

В настоящее время все более актуальной становится проблема защиты конфиденциальной информации, передаваемой по общественным сетям, ввиду повсеместного распространения сетевых технологий. Для решения данной проблемы необходимо осуществлять множество действий по обеспечению защиты информации. Наиболее важными методами защиты являются шифрование трафика и межсетевое экранирование на пограничных узлах сети, данные методы должны применяться в совокупности с организационными мерами защиты на предприятиях.

Одним из вариантов реализации такой системы защиты информации является система защиты и контроля сетевого трафика, представляющая собой совокупность схемы шифрования и механизма межсетевого экранирования, встроенных в маршрутизатор, которая располагается на территории организации.

Так как система защиты и контроля трафика предназначена для обеспечения защиты конфиденциальной информации, передаваемой по IP-сетям, был предложен вариант реализации данной системы, состоящий из

маршрутизатора с реализованной в нем системой защиты и контроля сетевого трафика, алгоритмы работы которой рассматриваются в представленной работе.

Информация, обрабатываемая в данном устройстве, соответствует грифу «конфиденциальная информация». Система защиты и контроля сетевого трафика представляет собой программно-аппаратный комплекс, состоящий из СКЗИ класса КС1 и межсетевого экрана уровня узла сети.

Таким образом, обобщенная постановка задачи - разработать алгоритмы функционирования и применения механизмов защиты, реализованных в системе защиты и контроля сетевого трафика, для информации с грифом не выше «конфиденциально».

1.2 Сеть как объект защиты информации

1.2.1 Общие сведения

Компьютерная сеть - это совокупность ПК и сетевого оборудования, объединяемых вместе с помощью сетевых кабелей таким образом, что они могут взаимодействовать друг с другом с целью совместного использования информации и ресурсов. Такое взаимодействие осуществляется в рамках реализованных сетевых протоколов.

IP-сеть – сеть, построенная на базе стека протоколов TCP/IP.

Стек протоколов TCP/IP - набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет. Название TCP/IP происходит из двух наиважнейших протоколов семейства - (TCP и IP, которые были разработаны и описаны первыми в данном стандарте. Также изредка упоминается как модель DOD в связи с историческим происхождением от сети ARPANET из 1970 годов (под управлением DARPA, Министерства обороны США).

Стек протоколов TCP/IP включает в себя четыре уровня:

- прикладной уровень;

- транспортный уровень;
- сетевой уровень;
- канальный уровень.

1.2.2 Прикладной уровень

На прикладном уровне работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), SSH (безопасное соединение с удалённой машиной), DNS (преобразование символьных имён в IP-адреса) и многие другие.

В основном эти протоколы работают поверх TCP или UDP и привязаны к определённому порту:

- HTTP на TCP-порт 80 или 8080;
- FTP на TCP-порт 20 (для передачи данных) и 21 (для управляющих команд);
- SSH на TCP-порт 22;
- запросы DNS на порт UDP (реже TCP) 53;
- обновление маршрутов по протоколу RIP на UDP-порт 520.

Эти порты определены Агентством по выделению имен и уникальных параметров протоколов (IANA). К этому уровню относятся: DHCP, Echo, Finger, Gopher, HTTP, HTTPS, IMAP, IMAPS, IRC, NNTP, NTP, POP3, POPS, QOTD, RTSP, SNMP, SSH, Telnet, XDMCP.

1.2.3 Транспортный уровень

Протоколы транспортного уровня могут решать проблему негарантированной доставки сообщений, а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

Протоколы автоматической маршрутизации, логически представленные на этом уровне (поскольку работают поверх IP), на самом деле являются частью протоколов сетевого уровня; например, OSPF (IP идентификатор 89).

TCP (IP идентификатор 6) - «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надёжный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности. В этом его главное отличие от UDP.

UDP (IP идентификатор 17) протокол передачи датаграмм без установления соединения. Также его называют протоколом «ненадёжной» передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. В приложениях, требующих гарантированной передачи данных, используется протокол TCP.

UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднён или не оправдан, либо в приложениях вида запрос-ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

И TCP, и UDP используют для определения протокола верхнего уровня число, называемое портом.

1.2.4 Сетевой уровень

Сетевой уровень изначально разработан для передачи данных из одной (под)сети в другую. Примерами такого протокола является X.25 и IP в сети ARPANET.

С развитием концепции глобальной сети в уровень были внесены дополнительные возможности по передаче из любой сети в любую сеть, независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удалённой стороны, например, в протоколе ICMP (используется для передачи диагностической информации IP-соединения) и IGMP (используется для управления multicast-потоками).

ICMP и IGMP расположены над IP и должны попасть на транспортный уровень, но функционально являются протоколами сетевого уровня, и поэтому их невозможно вписать в модель OSI.

Пакеты сетевого протокола IP могут содержать код, указывающий, какой именно протокол следующего уровня нужно использовать, чтобы извлечь данные из пакета. Это число - уникальный IP-номер протокола. ICMP и IGMP имеют номера, соответственно, 1 и 2.

К этому уровню относятся: DVMRP, ICMP, IGMP, MARS, PIM, RIP, RIP2, RSVP.

1.2.5 Канальный уровень

Канальный уровень (Link layer) описывает, каким образом передаются пакеты данных через физический уровень, включая кодирование (то есть специальные последовательности бит, определяющих начало и конец пакета данных). Ethernet, например, в полях заголовка пакета содержит указание того, какой машине или машинам в сети предназначен этот пакет.

Примеры протоколов канального уровня — Ethernet, IEEE 802.11 Wireless Ethernet, SLIP, Token Ring, ATM и MPLS.

PPP не вписывается в такое определение, поэтому обычно описывается в виде пары протоколов HDLC/SDLC. MPLS занимает промежуточное положение между канальным и сетевым уровнем и его нельзя отнести ни к одному из них. Канальный уровень иногда разделяют на 2 подуровня — LLC и MAC. Кроме того, канальный уровень описывает среду передачи данных (будь то

коаксиальный кабель, витая пара, оптическое волокно или радиоканал), физические характеристики такой среды и принцип передачи данных (разделение каналов, модуляцию, амплитуду сигналов, частоту сигналов, способ синхронизации передачи, время ожидания ответа и максимальное расстояние).

2 Обзор существующих механизмов защиты, применяемых в IP-сетях

2.1 Общие сведения

Передача информации в сети производится пакетами. Каждый пакет содержит служебные данные передающего и принимающего устройств, что позволяет осуществлять информационный обмен между устройствами.

Сетевое оборудование, в частности маршрутизатор является наиболее часто атакуемой частью сети, ввиду того, что имеет множество связей с другими маршрутизаторами и/или коммутаторами, а также является основным управляющим звеном в сетевом взаимодействии.

Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и несанкционированного доступа (НСД) к информации могут применяться следующие методы защиты (защитные механизмы):

- тестирование работоспособности основных узлов и модулей (предпусковой контроль);
- аутентификация (подтверждение подлинности) субъектов доступа;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- регистрация и оперативное оповещение о событиях, происходящих в системе и имеющих отношение к безопасности;
- криптографическое закрытие хранимых и передаваемых по каналам связи данных;
- контроль целостности сетевых пакетов;
- изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрывание внутренней структуры и адресации путем трансляции адресов);
- контроль целостности программного обеспечения;
- механизм защиты от несанкционированного доступа;

- обнаружение и противодействие атакам (опасным действиям нарушителей).

Перечисленные механизмы защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты. Помимо перечисленных могут применять и другие меры защиты или различные их модификации.

2.2 Предпусковой контроль

Механизм обеспечивает безопасную загрузку устройства. При корректной реализации механизма не представляется возможным внедрение несанкционированных изменений в программное обеспечение или модификация аппаратной части. Механизм предпускового контроля включает в себя:

- контроль питающих напряжений;
- контроль корректности работоспособности ОЗУ;
- контроль корректности работоспособности АЛУ;
- контроль корректности шины адреса;
- механизм самотестирования модулей системы.

Совокупность данных методов защиты позволяет осуществить безопасную загрузку системы, исключить возможность несанкционированного вмешательства в процесс загрузки и перейти в режим работы без компрометации информации. Предпусковой контроль включает в себя разносторонние тесты АЛУ, ОЗУ, ПЗУ, специфические тесты для системы (разрабатываются проектировщиками). Набор тестов для каждой разрабатываемой системы определяется разработчиком и согласуется с заказчиком при необходимости.

2.3 Аутентификация субъектов доступа

Механизм аутентификации субъектов позволяет подтвердить наличие прав доступа у субъекта доступа, при этом данный механизм может быть реализован многими способами, наиболее распространёнными являются:

- сопоставление отпечатков пальцев;
- сопоставление узора радужной оболочки глаза и структуры сетчатки глаза;
- предъявление токенов, карт доступа и других аутентифицирующих пользователя носителей;
- использование парольно-кодовых методов.

Аутентификация может использоваться как для администраторов, так и для рядовых пользователей, при этом даже в однопользовательских системах необходима реализация данного механизма для исключения факта ложной идентификации администратора, а также внесения несанкционированных изменений в конфигурацию с использованием прав доступа администратора.

2.4 Разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям

Целью разграничения доступа к информации в первую очередь является предотвращение реализации угрозы нарушения конфиденциальности или несанкционированного доступа к информации.

Объект - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Субъект - лицо или процесс, действия которого регламентируются правилами разграничения доступа

Доступ к информации - ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации.

Корректная реализация данного механизма обеспечивает однозначную идентификацию субъекта доступа в процессе выполнения им доступа к объекту информационной системы. Необходимость использования данного механизма обуславливается распространенностью атак типа «социальная инженерия», а также наличием внутреннего нарушителя и возможностью сговора персонала со злоумышленниками.

Механизмы управления доступом субъектов к объектам доступа выполняют основную роль в обеспечении внутренней безопасности компьютерных систем. Данные механизмы имеют множество вариантов реализаций, но наиболее распространенный и простой для использования и поддержки является механизм дискреционного управления доступом.

Авторизация (присвоение полномочий пользователям) осуществляется администратором системы, в результате данной процедуры формируются учетные записи пользователей со списками доступа с перечнем атрибутов доступа (например, доступ на чтение/ на запись и т.д.). После формирования списка учетных записей пользователей администратор назначает пользователям системы учетную запись в соответствии с определенными полномочиями.

Также авторизация необходима для самого администратора, а при использовании однопользовательских систем, где единственный пользователь – администратор такая процедура является обязательной.

2.5 Регистрация и оперативное оповещение о событиях, происходящих в системе и имеющих отношение к безопасности

Данный механизм применяется для осуществления мониторинга информационной безопасности в системе, отслеживания и отладки неисправностей и сбоев системы, сбор статистики работы для модификации или ремонта устройств.

Перечень регистрируемых событий определяется на этапе разработки системы и дополняется на этапах тестирования, отладки, лицензирования и

сертификации (при необходимости). В основном осуществляют регистрацию следующих событий:

- вход пользователя в систему;
- вход администратора в систему;
- включение;
- выключение;
- изменение конфигурации;
- ошибка входа пользователя в систему;
- ошибка входа администратора в систему;
- запрет доступа к объекту;
- доступ к объекту.

Данный перечень позволяет отследить большинство потенциально-опасных событий системы и принять соответствующие меры.

Также при определении перечня регистрируемых событий для некоторых из них могут определяться сигналы оповещения, как для особо важных событий. Сигнал оповещения в основном представляет собой светодиодную индикацию со звуковым (локальное оповещение) и посылку пакета информации с кодом события на пульт управления (дистанционное оповещение).

Одной из приобретающих популярность в настоящее время разновидностью сигнала дистанционного оповещения является автоматическая передача SMS через мобильную связь ответственному за безопасность лицу с кратким описанием произошедшего события.

2.6 Криптографическое закрытие хранимых и передаваемых по каналам связи данных

Основным криптографическим преобразованием, применяемым для закрытия данных, является – шифрование.

Шифрование – универсальный способ защиты информации, циркулирующей в канале связи и устройствах обработки, позволяющий

защититься от НСД к информации, несанкционированного копирования, а также от ряда сетевых компьютерных атак:

- IP/TCP фрагментация;
- IP spoofing;
- ARP-spoofing;
- переполнение буфера;
- атаки типа «вставка по середине».

Для реализации данного механизма защиты существует два наиболее распространенных подхода – использование VPN или специального стека протоколов IPSec.

VPN – это безопасное, зашифрованное подключение между двумя сетями или между отдельным пользователем и сетью. Сети VPN позволяют пользоваться интернетом, сохраняя конфиденциальность.

VPN можно классифицировать по следующим параметрам:

- по степени защищённости используемой среды (все данные зашифрованы или просто создана частная сеть);
- по способу реализации (программное решение или интегрированное);
- по назначению;
- по типу протокола (TCP/IP, IPX и AppleTalk);
- по уровню сетевого протокола (на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI);
- по доступу.

Соединение с VPN называется «туннелем», туннель создаётся на основе подключения к интернету. Туннель - это подключение между двумя абонентами с использованием инкапсуляции пакетов данных. Оба компьютера, в свою очередь, называются узлами. Каждый из узлов отвечает за степень защищённости соединения до того, как они попадут в туннель.

IPSec – комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов, в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC.

Архитектура IPSec представлена на рисунке 1.

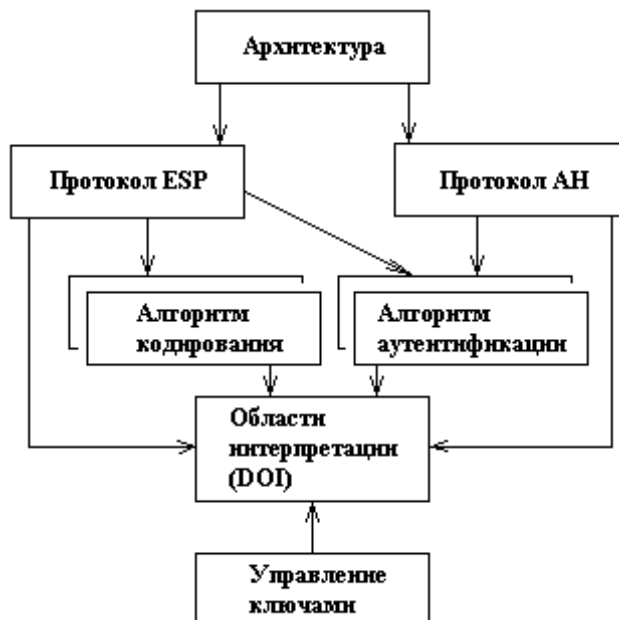


Рисунок 1 – Архитектура IPSec

Основные преимущества IPSec:

- полная прозрачность не только для приложений, но и маршрутизаторов, драйверов сетевых карт и так далее. С точки зрения логики работающей программы или устройства - ведется передача обычных пакетов, использование IPSec незаметно;
- шифрование трафика с помощью IPSec в небольшой локальной сети не влечет потерю производительности;
- высокий уровень управляемости - систему можно применять к трафику отдельно взятых компьютеров или даже программ, настройка производится в разделе политик IPSec.

2.7 Контроль целостности сетевых пакетов

Контроль целостности и аутентичности информации, передаваемой с использованием сетевых технологий является классическим методом защиты

информации от несанкционированного изменения, ошибок при передаче, искажения и т.д. Данный метод функционирует следующим образом:

- на сформированный пакет осуществляется расчёт контрольной суммы;
- рассчитанное значение КС записывается в соответствующее поле заголовка IP-пакета;
- осуществляется отправка пакета в канал связи;
- на приемной стороне осуществляется подтверждение корректности контрольной суммы.

Из-за известности алгоритмов расчета контрольных сумм они применяются в качестве проверки целостности и аутентичности информации только совместно с шифрованием, когда значение контрольной суммы, рассчитанной общеизвестным алгоритмом, а потому легко подменяемой, становится закрытым от внешнего доступа. При отсутствии шифрования в системе информационной безопасности для проверки целостности и аутентичности используются более сложные механизмы, (например, ЭЦП).

2.8 Изоляция (защита периметра) компьютерных сетей (скрытие внутренней структуры и адресации путем трансляции адресов)

Network Address Translation – трансляция (подмена) сетевых адресов. Эта технология позволяет с одной стороны, противостоять нехватке IPv4 адресов, а с другой – повысить защищённость сети.

Для того чтобы организовать возможность выхода в интернет с устройств, имеющих приватные адреса применяется технология трансляции адресов, либо используется прокси-сервер. Если попытаться отправить, например, запрос к веб-серверу, находящемуся в интернете, с приватного адреса, то сам запрос теоретически дойдёт, так как веб сервер имеет публичный адрес, а ответ от сервера не вернётся, так как обратный адрес, на который этот ответ надо слать – приватный. Трансляция адресов заключается в том, что есть некоторое NAT-

устройство, например, сервер или маршрутизатор, который имеет один или несколько публичных адресов. Клиенты с приватными адресами пытаются отправить запросы напрямую получателю в интернете, но IP пакеты по пути попадают на такое устройство. При этом в пакете подменяется адрес отправителя: вместо приватного адреса клиента, устройство ставит в это поле один из своих публичных адресов, после чего пакет отправляется в сеть. Получатель обрабатывает пакет и возвращает на него ответ (например, содержимое запрошенной из интернета странички). Этот ответ, идёт на публичный адрес устройства, занимающегося NAT-ом. Устройство помнит, когда и какой адрес оно подменяло и в этом пакете адрес получателя снова меняется: публичный адрес устройства заменяется на приватный адрес клиента, после чего пакет идёт дальше во внутреннюю сеть.

2.9 Контроль целостности программного обеспечения

Контроль целостности программного обеспечения - это механизм, необходимый для отслеживания неизменности файлов, документов, реестра, конфигурации оборудования системы.

Данный механизм может применяться для отслеживания и контроля эталонного состояния средства обработки информации.

Каждый тип объектов имеет свой набор контролируемых данных. Так, например, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие по заданному пути. Кроме того, для каждого из типов объектов могут использоваться различные алгоритмы контроля целостности.

В системе может быть предусмотрено множество различных видов реализации подсистемы контроля целостности. В частности, контроль может быть выполнен при загрузке ОС, при входе или выходе пользователя из системы, по заранее составленному расписанию. Кроме того, может быть проведен и немедленный контроль.

При обнаружении несоответствия возможны следующие реакции подсистемы контроля целостности на возникающие ситуации:

- регистрация изменений в журнале безопасности;
- блокировка компьютера;
- отклонение или принятие изменений.

Для каждого типа контролируемых объектов хранится список имен объектов и задания для контроля тех или иных характеристик указанных объектов. Эта информация размещается в базе данных подсистемы контроля целостности, которая реализована в виде набора файлов определенного формата, расположенных в отдельном каталоге. Задание на контроль содержит необходимую информацию об эталонном состоянии объекта, порядке контроля характеристик и действий, которые надо выполнить при обнаружении изменений. Результаты контроля и обработки запросов фиксируются в журнале регистрации событий.

2.10 Механизм защиты от несанкционированного доступа

Существует множество методов, с помощью которых злоумышленники получают несанкционированный доступ к конфиденциальной информации. В целом все способы можно разделить на четыре основные группы:

- несанкционированный доступ внешним нарушителем при наличии физического доступа к компьютеру;
- несанкционированный доступ к информации при ее передаче за пределы контролируемой зоны;
- утечка информации, вызванная внутренним нарушителем, имеющим легитимный доступ к данным;
- удаленное проникновение на компьютер и похищение данных с помощью эксплуатации уязвимостей или использования вредоносного программного обеспечения.

В первом случае нарушитель, не являющийся пользователем рабочего места, но имеющий физический доступ к компьютеру с конфиденциальной информацией, может выполнить различные локальные атаки, например, загрузку с внешнего носителя и копирование информации с жесткого диска, или совершить кражу носителей информации. Данная угроза имеет наибольшую актуальность для организаций, работающих в сфере услуг и обслуживания. В таких компаниях открыт свободный доступ для посетителей, и злоумышленник может отвлечь оператора или использовать один из свободных компьютеров для проведения атаки. Если же говорить о краже — от данной угрозы не защищена ни одна компания. Известно много случаев, когда ограбление планировалось с одной целью — похитить жесткие диски с ценными коммерческими данными. Для защиты от нежелательных манипуляций злоумышленника с компьютерами можно использовать разные подходы. Классическим методом является физическая защита портов ввода-вывода, использование аппаратных плат доверенной загрузки и другие сложные меры, которые требуют существенных затрат и тормозят бизнес-процессы. Криптографические средства могут решить эту проблему проще, обеспечив полное шифрование данных на жестких дисках и предоставляя доступ пользователю только после надежной аутентификации. Дополнительно данный способ защиты позволит нивелировать угрозу кражи носителей — злоумышленник не сможет прочесть информацию с похищенного жесткого диска.

Второй случай — несанкционированный доступ при передаче информации за пределы контролируемой зоны — очень обширен из-за наличия большого числа возможных каналов передачи. Данные могут передаваться через глобальные сети по различным протоколам и через множество сервисов. Существует масса видов атак и угроз — перехват трафика, подделка адресов, взлом сервисов хранения файлов и так далее. Все эти угрозы находятся за пределами защищаемого периметра и средства защиты могут только блокировать передачу данных, но не могут обеспечить их безопасность. Кроме того, информацию за пределы периметра могут выносить с помощью съемных

носителей — дисков, флеш-накопителей, внешних жестких дисков, — и эти данные также нельзя контролировать. Единственный способ сохранить конфиденциальные данные в тайне — использовать криптографические преобразования, чтобы защитить информацию от НСД и позволить работать с ней только легитимному получателю данных. В остальных случаях криптографическая защита бессильна — шифрование не может обеспечить защиту от утечки информации со стороны пользователя, имеющего легитимный доступ к данным.

2.11 Обнаружение и противодействие атакам (опасным действиям нарушителей)

Основной целью данного механизма защиты является обнаружение и предотвращение несанкционированных действий в информационной системе.

Для обеспечения конфиденциальности, целостности и доступности информации строят эшелонированные системы защиты. Функциональность привычных средств защиты информации, например, межсетевого экрана и антивируса, дополняется системами обнаружения вторжений. СОВ предоставляют администратору полную информацию о событиях информационной безопасности в сети, а значит, и полную картину об информационных потоках в сети. Понятная и детализированная картина событий позволяет администратору построить гибкую и эффективную систему защиты.

СОВ позволяет обнаружить:

- попытки вторжения в сеть;
- вирусы;
- внутренних злоумышленников;
- запрещенный пользовательский трафик.

Структура СОВ представлена на рисунке 2.

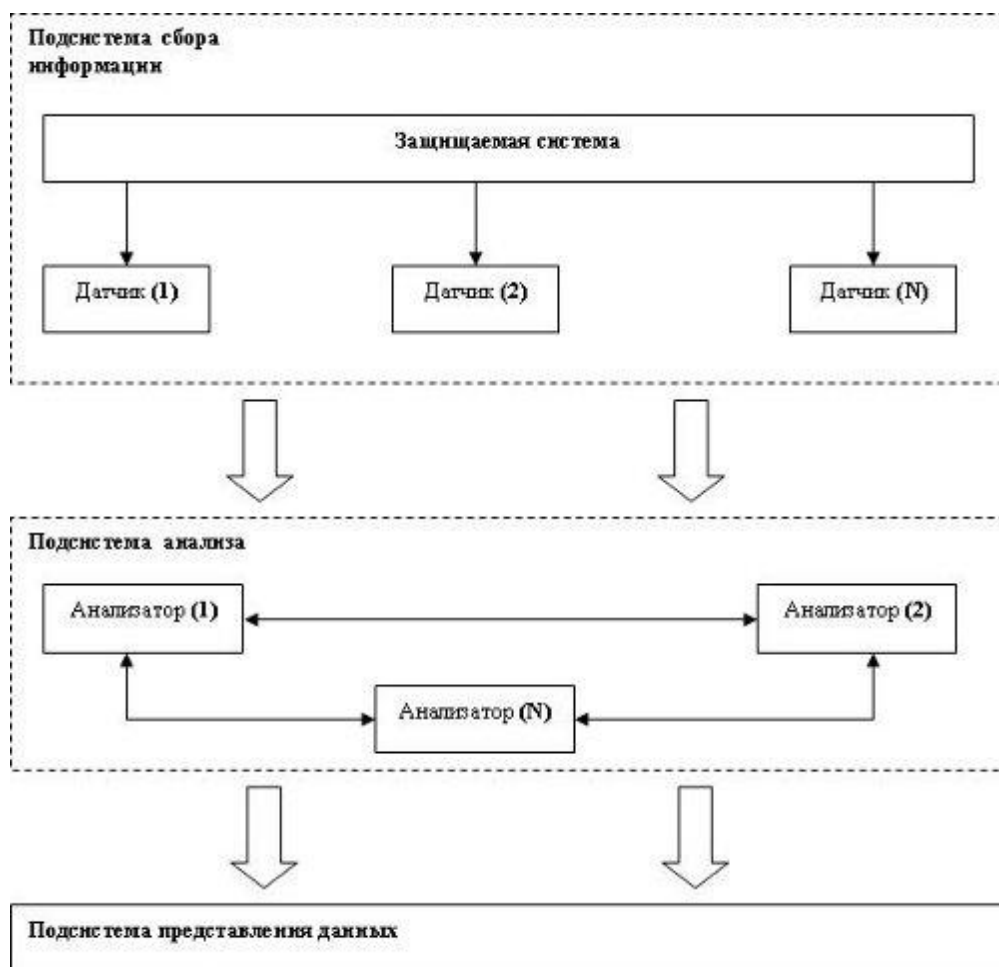


Рисунок 2 – Структура СОВ

Подсистема сбора информации аккумулирует данные о работе защищаемой системы. Для сбора информации используются автономные модули – датчики. Количество используемых датчиков различно и зависит от специфики защищаемой системы.

Подсистема анализа структурно состоит из одного или более модулей анализа – анализаторов. Наличие нескольких анализаторов требуется для повышения эффективности обнаружения. Каждый анализатор выполняет поиск атак или вторжений определенного типа. Входными данными для анализатора является информация из подсистемы сбора информации или от другого анализатора. Результат работы подсистемы – индикация о состоянии защищаемой системы. В случае, когда анализатор сообщает об обнаружении несанкционированных действий, на его выходе может появляться некоторая

дополнительная информация. Обычно эта информация содержит выводы, подтверждающие факт наличия вторжения или атаки.

Подсистема представления данных необходима для информирования заинтересованных лиц о состоянии защищаемой системы. В некоторых системах предполагается наличие групп пользователей, каждая из которых контролирует определенные подсистемы защищаемой системы. Поэтому в таких СОВ применяется разграничение доступа, групповые политики, полномочия и т.д.

СОВ может быть реализована программным, аппаратным и организационным способом, при этом также возможно совмещение различных способов.

3 Разработка архитектуры системы связи организации с учетом системы защиты и контроля сетевого трафика

3.1 Место СЗИКСТ в системе связи организации

Система защиты и контроля трафика расположена в сети, в составе комплекса средств ЗИ, циркулирующей в сетях конфиденциальной связи с использованием сетевых технологий, и размещается непосредственно между переходом от внешней сети к внутренней сети организации, и реализуется на пограничном маршрутизаторе.

Общая схема организации связи с использованием средств защиты информации, циркулирующей в сетях конфиденциальной связи, приведена на рисунке 3. Объект исследования представляет собой промежуточный узел между внешней IP-сетью и маршрутизатором предприятия, при этом физически СЗИКСТ и маршрутизатор являются одним целым (СЗИКСТ является аппаратно-программным решением для маршрутизатора).

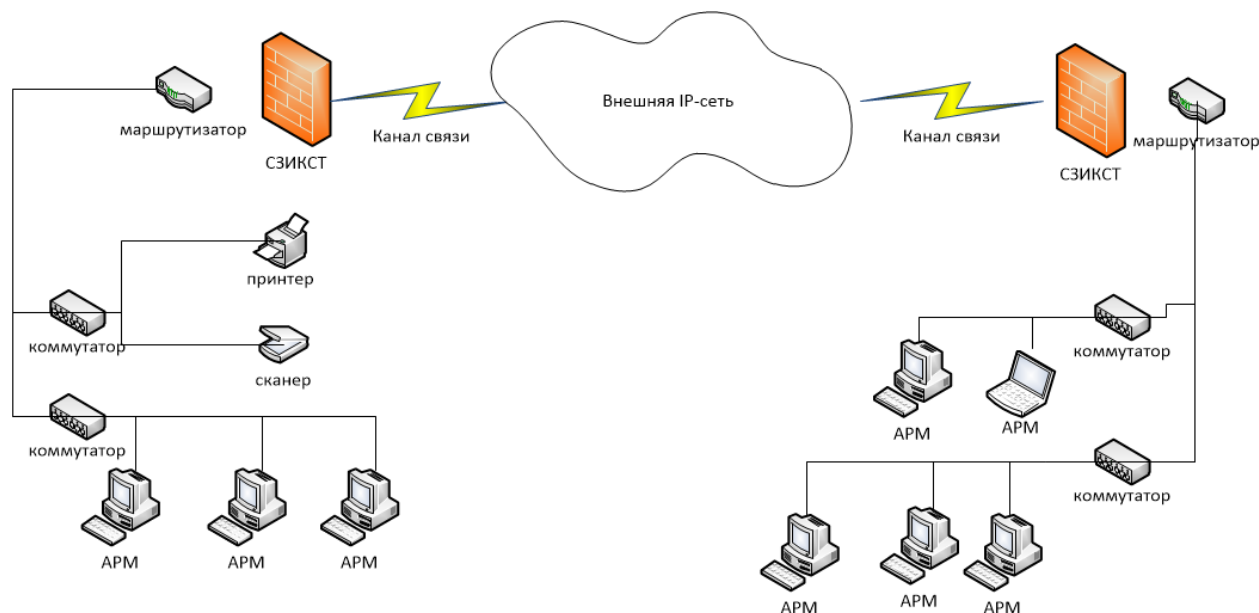


Рисунок 3 – Место объекта исследования в сети связи

СЗИКСТ, обеспечивающая защиту конфиденциальной информации, циркулирующей в сети связи организации, предназначена для:

- защиты информации внутренней сети предприятия от деструктивных воздействий со стороны абонентских каналов IP/MPLS сетей;
- организации 10 защищенных каналов связи по протоколу IEEE 802.3;
- защиты от НСД и сетевых компьютерных атак оборудования внутренней сети предприятия (коммутационного, абонентского сетевого, абонентского терминального оборудования);
- непрерывной криптографической аутентификации IP-пакетов, передаваемых между абонентами и узлами сети предприятия.

СЗИКСТ совместно с организационными мерами защиты информации обеспечивает безопасный информационный обмен между подсетями организации и внешней сетью, позволяет сформировать криптографически защищенный туннель между аналогичными устройствами.

К организационным мерам защиты, реализуемым на территории функционирования системы защиты и контроля сетевого трафика, относятся:

- ограничение доступа в помещения посторонних лиц или сотрудников других подразделений;
- жёсткое ограничение круга лиц, имеющих доступ к каждому компьютеру;
- формирование контролируемой зоны организации;
- создание контрольно – пропускных пунктов;
- проведение повышения квалификации персонала в области ИБ;
- наличие и соблюдение корпоративной политики ИБ.

3.2 Криптографическая защита комплекса

3.2.1 Основные положения

Криптографическая защита комплекса реализуется в соответствии со стандартом ГОСТ 28147-89. В маршрутизаторе имеется встроенная схема шифрования, расположенная таким образом, что пакеты данных, принятые из

внешней сети (порты WAN) после обработки попадают на схему шифрования, затем осуществляется расшифрование принятых пакетов и их анализ по содержанию механизмом межсетевого экранирования. После чего при получении положительных результатов работы механизма межсетевого экранирования пакет направляется на порты внутренней сети (порты LAN) маршрутизатора. Схожим образом происходит и формирование пакета для внешней сети, на маршрутизаторе принятый из внутренней сети не зашифрованный IP-пакет попадает на схему шифрования, после чего осуществляется его зашифрование, инкапсуляция в ESP-пакет и отправка в один из каналов связи.

3.2.2 Описание криптографической схемы

Криптографическая схема защиты информации должна представлять собой совокупность следующих элементов:

- ключи парно-выборочной конфиденциальной связи $K_k(i,j)$ и их ключи хранения $K_{хр-к}(i)$. Ключ $K_k(i,j)$ предназначен для генерации сеансового ключа связи для встречной работы криптомаршрутизатора с криптономером i и криптомаршрутизатора с криптономером j . Ключи $K_k(i,j)$ входят в состав ключевого блокнота, который вводится в криптомаршрутизатор с портативного носителя. Ключи $K_k(i,j)$ записаны на носитель в зашифрованном и имитозащищенном виде на ключе $K_{хр-к}(i)$. В качестве алгоритма шифрования используется криптоалгоритм ГОСТ 28147-89. Ключ $K_{хр-к}(i)$ записан на носитель в маскированном виде;
- вектор инициализации ПДСЧ $КДСЧ(i)$. Вектор $КДСЧ(i)$ предназначен для начальной инициализации датчика случайных чисел. Вектор $КДСЧ(i)$ входит в состав ключевого блокнота. Вектор $КДСЧ(i)$ записан на носитель в маскированном виде;
- таблица узлов замены для криптоалгоритма ГОСТ 28147-89. Таблица предназначена для использования в алгоритме ГОСТ 28147-89 при работе

криптомаршрутизатора в сети конфиденциальной связи. Таблица входит в состав ключевого блокнота;

- маска $M_{кр-к(i)}$ ключа хранения $K_{кр-к(i)}$. Предназначена для маскирования ключа хранения $K_{кр-к(i)}$;
- маска $МДСЧ(i)$ вектора $КДСЧ(i)$. Предназначена для маскирования вектора инициализации $ПДСЧ КДСЧ(i)$.

В ключевую структуру изделия также должны входить производные ключи – сеансовые и пакетные, и ключ защиты от НСД и проверки целостности ПО.

Обмен информацией между парой аппаратов необходимо осуществлять в виде сеансов связи. В процессе установления сеанса аппараты создают сеансовые ключи на основе общего индивидуального ключа.

Одновременно создается четыре сеансовых ключа:

- ключ шифрования в одну сторону (от инициатора к респонденту);
- ключ шифрования в противоположную сторону (от респондента к инициатору);
- ключ имитозащиты в одну сторону (от инициатора к респонденту);
- ключ имитозащиты в противоположную сторону (от респондента к инициатору).

Сеансовые ключи шифрования используются для создания пакетных ключей. Один сеансовый ключ используется для создания не более 128 пакетных ключей. При достижении максимального допустимого значения счетчика созданных пакетных ключей сеанс закрывается (удаляются сеансовые ключи шифрования и имитозащиты), и организуется новый сеанс (создаются новые сеансовые ключи шифрования и имитозащиты). Для обеспечения непрерывности связи новый сеанс создается заранее, когда счетчик созданных пакетных ключей предыдущего сеанса еще не исчерпан полностью.

Сеансовые ключи имитозащиты используются для имитозащиты служебных пакетов, передаваемых в процессе установления соединения, а также для имитозащиты служебных полей пакетов данных. После создания сеансовые

ключи сохраняются в оперативной памяти аппарата под масками. При выключении питания сеансовые ключи теряются.

Пакетные ключи создаются на основе сеансовых ключей шифрования и используются для зашифровывания/расшифровывания пакетов данных. Каждый пакетный ключ используется для зашифровывания только одного пакета данных размером не более 1300 байт. Пакетные ключи создаются кратковременно (на время зашифровывания/расшифровывания пакета) и удаляются после однократного использования.

3.2.3 Генератор псевдослучайной последовательности

Составной частью системы защиты и контроля трафика является генератор псевдослучайных чисел, выполненный программным способом в модуле управления. Выработанная псевдослучайная последовательность, используется для:

- формирования новой маски ключа хранения индивидуальных ключей;
- формирования масок, используемых для закрытия информации на пути от схемы шифрования до блока коммутатора пакетов WAN/LAN и от блока коммутатора пакетов WAN/LAN до узла аппаратного шифрования.

ПДСЧ реализован с использованием алгоритма ГОСТ 28147-89 в режиме гаммирования. В качестве ключа и синхропосылки для алгоритма ГОСТ используется случайная последовательность (производный ключ инициализации ДСЧ и производная синхропосылка, полученные в предыдущем цикле работы ПДСЧ), хранящаяся в узле хранения КИ.

При первоначальной инициализации ПДСЧ используется случайная последовательность, считанная с ключевого блокнота, и нулевая синхропосылка.

Выработка СП в процессе работы ПДСЧ производится в модуле управления с использованием ключа инициализации и синхропосылки, которые берутся из узла хранения КИ. Выработанные СП анализируются с точки зрения

соответствия их статистических параметров эталонным. В случае, когда статистические характеристики последовательностей удовлетворяют заданному критерию, из них формируются новые значения ключа и синхропосылки, которые сохраняются в узле хранения КИ. Оставшаяся часть СП используется по назначению в качестве синхропосылок при шифровании пакетов.

4.2 Механизм аутентификации

Данный механизм позволяет однозначно определить субъект доступа. Учитывая, что проектируемая система является однопользовательской, необходимо выполнять только аутентификацию администратора. Осуществляется данный процесс посредством ввода администратором логина и пароля в систему. Требования к паролю: мощность алфавита не менее 52 символов и длина не менее 10 символов.

В системе хранится только хэш пароля администратора, при этом активных (активированная учетная запись) администраторов системы защиты может быть не более 1. Аутентификация осуществляется только локально. Для подтверждения прав доступа администратору необходимо с использованием ПЭВМ подключиться по физическому интерфейсу 8P8C к любому разъему маршрутизатора, после чего в командной строке появится предложение ввода аутентификационных параметров. После прохождения процедуры аутентификации инициируется отсчет времени, в течении которого будет возможно внесение изменений в конфигурацию маршрутизатора – 10 минут. По истечении заданного промежутка времени меню управления администратора становится неактивным, доступ к функциям управления не возможен. Данная мера защиты необходима для исключения ошибочных действий администратора или покидания места расположения маршрутизатора в процессе конфигурирования.

Данный механизм позволяет защититься от несанкционированного доступа в систему посторонних лиц. Корректность реализации данного механизма обеспечивается наличием контролируемой зоны организации и квалификацией администратора. Алгоритм работы механизма аутентификации представлен на рисунке 5.

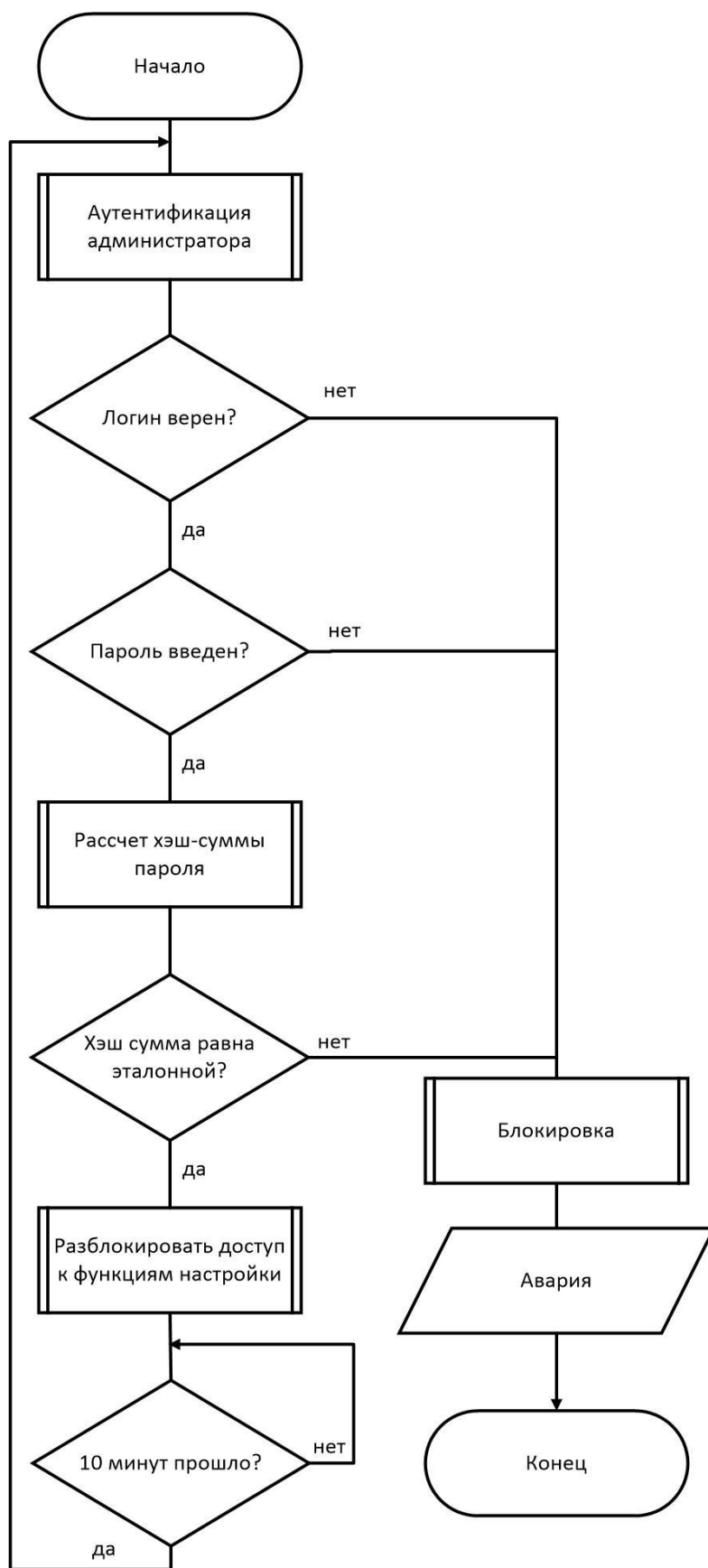


Рисунок 5 – Алгоритм работы механизма аутентификации администратора

4.3 Механизм предпускового контроля

Механизм предпускового контроля включает в себя:

- контроль питающих напряжений;
- контроль корректности работоспособности ОЗУ;
- контроль корректности работоспособности АЛУ;
- контроль корректности шины адреса;
- механизм самотестирования модулей системы.

Контроль питающих напряжений проводится при включении питания. В маршрутизаторе реализована схема контроля питающих напряжений, при этом схема контроля питания имеет независимый источник питания – аккумулятор. При поступлении напряжения на схему контроля питания она осуществляет съём значений напряжения подаваемого на модули системы, после чего передает полученные значения в АЦП, данные принятые АЦП передаются в качестве параметров в функцию контроля питания. В данной функции осуществляется сравнение с эталонным значением напряжения питания для каждого из модулей системы, после чего при получении корректных результатов контроля питания осуществляется дальнейшее тестирование системы, а при получении отрицательных результатов осуществляется подача питания на схему сброса, данная схема осуществляет сброс настроек модулей системы и сигнализацию об аварии.

Данный механизм позволяет подтвердить корректность уровня напряжения питания для недопущения его падения или повышения, приводящего к не отслеживаемым последствиям. Реализация данного механизма обеспечивается наличием схемы контроля питания и блокировки работы при получении отрицательных результатов тестирования.

Алгоритм работы механизма контроля питания представлен на рисунке 6.

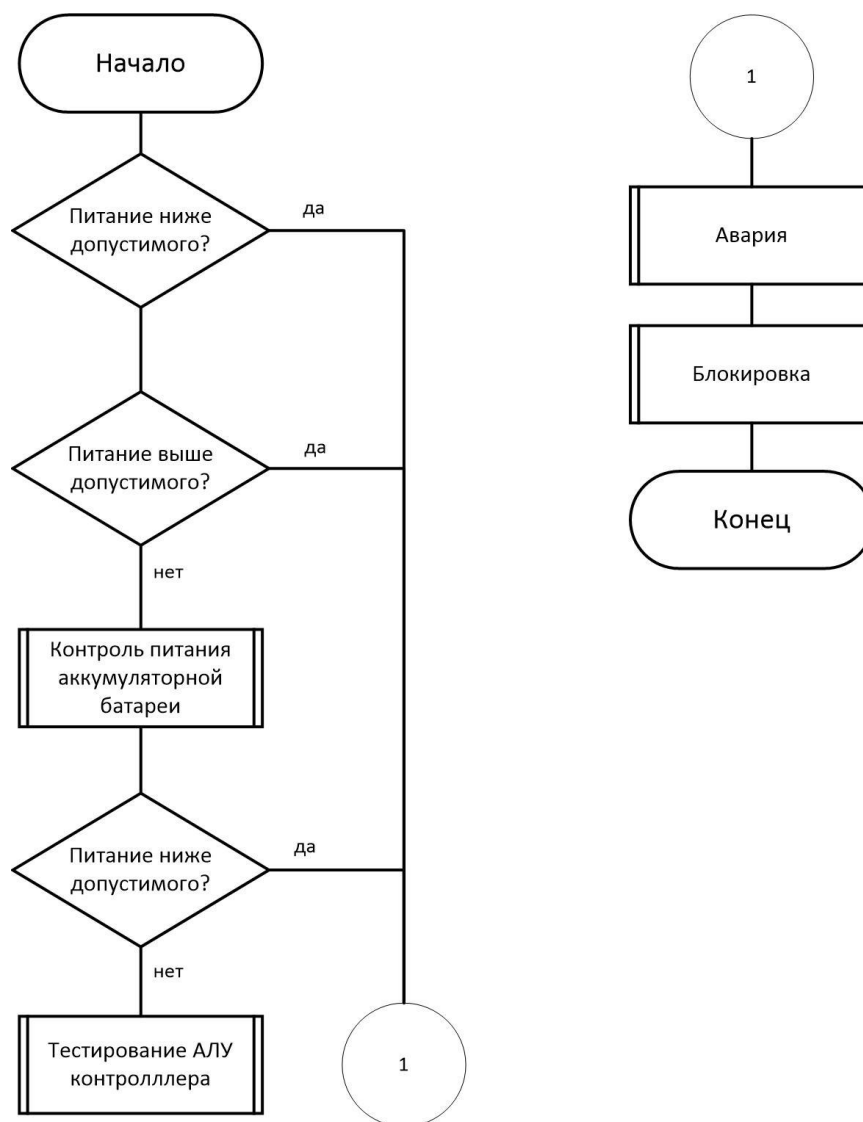


Рисунок 6 – Механизм контроля питания

Контроль корректности работоспособности ОЗУ осуществляется с использованием методов тестирования:

- проверка собственного адреса;
- проверка инвертированного адреса;
- бегающая единица;
- бегающий нуль.

Данные методы применяются последовательно, в случае возникновения ошибки при тестировании в любом из методов осуществляется блокировка работы до перезапуска.

Проверка собственного адреса осуществляется следующим образом:

- считывается адрес первой ячейки памяти в промежуточный буфер памяти;
- записывается считанный адрес ячейки в саму ячейку памяти;
- осуществляется сравнение значений в промежуточном буфере и записанного в ячейке памяти;
- если получен положительный результат сравнения проверяется следующая ячейка памяти.

Проверка инвертированного адреса осуществляется тем же образом, только к считанному адресу применяется инверсия.

Проверка с тестированием бегающей единицей:

- память заполняется нулями;
- побитно записывается и считывается единица.

Проверка с тестированием бегущим нулем:

- память заполняется нулями;
- побитно считывается ноль (значение по адресу ячейки памяти).

Перечисленные тесты проверяют функционирование как оперативной, так и постоянной памяти. Данный механизм позволяет подтвердить корректность работы ОЗУ и ПЗУ для недопущения несанкционированных ошибок в процессе работы. Реализация данного механизма обеспечивается наличием механизма тестирования памяти и блокирования работы при получении отрицательных результатов тестирования.

Контроль корректности работоспособности АЛУ осуществляется для подтверждения правильности функционирования арифметико-логических операций. Механизм контроля корректности работоспособности АЛУ представляет собой совокупность проверок следующих операций:

- сложение (ассемблерное ADD);
- вычитание (ассемблерное SUB);
- логическое И (ассемблерное OR);
- логическое ИЛИ (ассемблерное XOR);

- логическое НЕ (ассемблерное NOT);
- инкрементирование;
- декрементирование;
- арифметический сдвиг вправо/влево (ассемблерное SRA SLA);
- умножение (ассемблерное MUL);
- деление (ассемблерное SUB).

Проверка корректности данных операций проводится последовательно, при этом при наличии ошибки в любой из операций осуществляется блокировка работы с аварией.

Алгоритм работы механизма предпускового контроля АЗУ, ОЗУ, ПЗУ, шины адреса представлен на рисунке 7.

Механизм самотестирования модулей системы реализуется непосредственно в модуле управления и осуществляет опрос остальных модулей системы о результатах предпускового контроля, после чего собирает полученные результаты в двоичный вектор, где размер вектора определяется количеством модулей системы, в данный вектор устанавливается бит в состояние «1» при получении положительных результатов предпускового контроля, после чего модуль управления осуществляет побитовое сравнение сформированного вектора с эталонным значением (для системы защиты и контроля сетевого трафика вектор 111b ввиду наличия трех модулей), при получении отрицательных результатов механизма самотестирования модулей системы осуществляется блокировка работы и сигнализация об аварии.

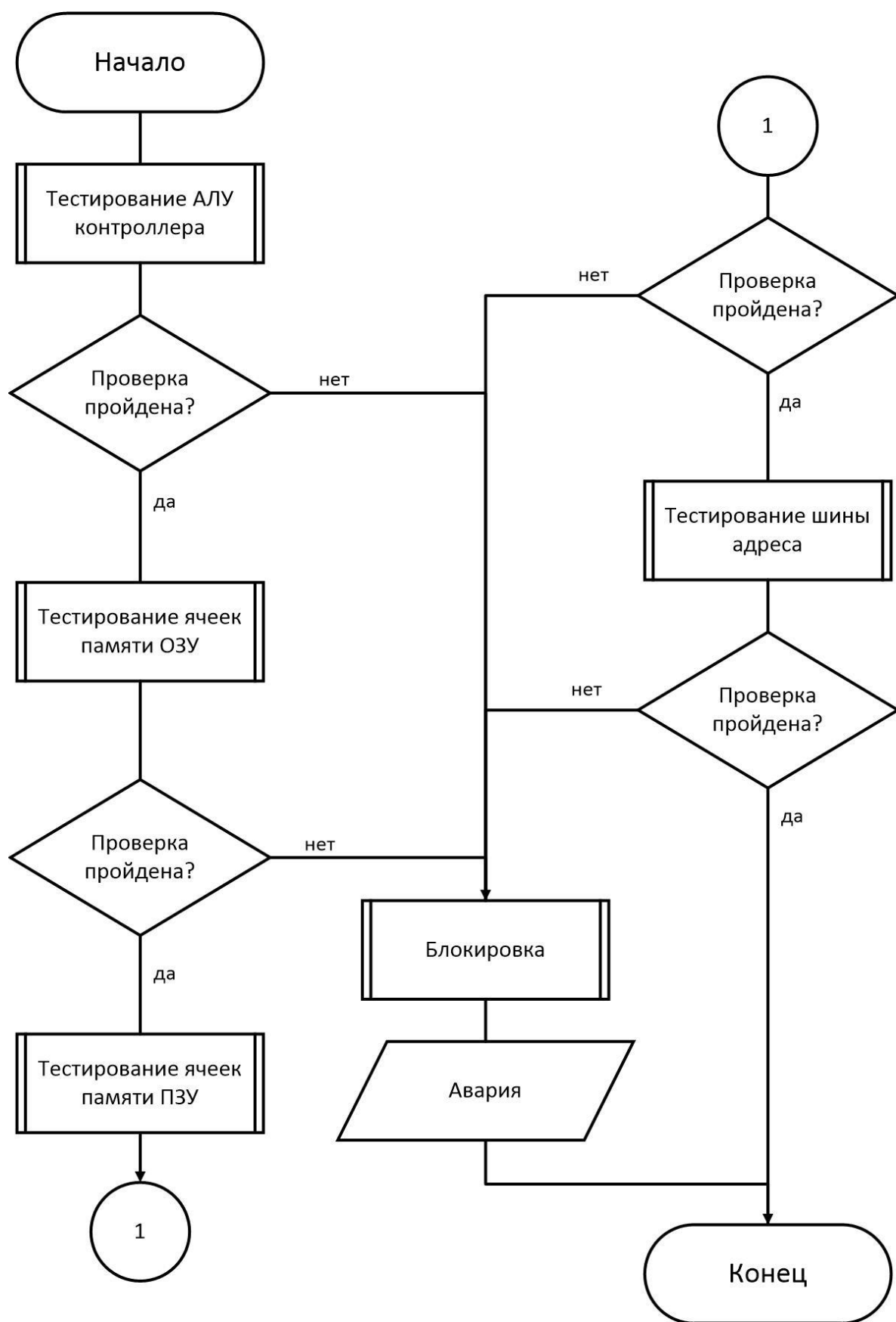


Рисунок 7 – Алгоритм работы механизма предпускового контроля АЗУ, ОЗУ, ПЗУ, шины адреса

4.4 Регистрация и оперативное оповещение о событиях, происходящих в системе и имеющих отношение к безопасности

Данный механизм позволяет оповестить оператора системы о несанкционированном вмешательстве в работу. Реализуется посредством светодиодной индикации и звукового оповещения. Также каждое событие системы (тип регистрируемых событий определяется РД) регистрируется в журнале событий. При возникновении событий, определенных «Правилами пользования...» или другими регламентирующими документами, осуществляется блокировка работы с оповещением о типе события, к опасным событиям могут быть отнесены:

- регистрация события НСД;
- ошибка целостности ПО;
- ошибка целостности ключевой информации.

Блокировка сбрасывается перезапуском системы.

4.5 Механизм контроля целостности программного обеспечения

Данный механизм позволяет отслеживать изменения в программном обеспечении. При запуске системы осуществляется расчёт контрольной суммы по алгоритму CRC32, после чего рассчитанное значение сравнивается с эталонным, хранящимся в ПЗУ маршрутизатора, при совпадении значений контрольных сумм осуществляется загрузка программного обеспечения в оперативную память маршрутизатора. При получении отрицательных результатов процесс запуска системы прекращается. Данный механизм запускается только после успешного прохождения механизма предпускового контроля, также при любом легитимном изменении параметров эталонное значение контрольной суммы может быть пересчитано, при этом необходимо пройти процедуру аутентификации администратора.

Несанкционированные изменения в ПО маршрутизатора могут быть внесены через USB разъем. Для избежания опасной ситуации, данный разъем закрыт крышкой, и имеет только один возможный субъект доступа – USB-носитель и идентификатором администратора, к которому у посторонних лиц доступа не имеется, любые другие носители USB не будут идентифицированы в системе и чтение данных с них будет невозможно.

Алгоритм работы механизма контроля целостности ПО представлен на рисунке 8.



Рисунок 8 – Алгоритм работы механизма контроля целостности программного обеспечения

4.6 Механизм защиты от несанкционированного доступа к внутренним элементам маршрутизатора

Данный механизм представляет из себя совокупность датчиков НСД, встраиваемых в корпус маршрутизатора и срабатывающих при вскрытии корпуса или при несанкционированном подключении к разъемам. При срабатывании датчиков НСД возникает сигнал, передаваемый на схему сброса питания. Сигнал сброса можно убрать только посредством проведения текущего ремонта.

Корпус маршрутизатора имеет разъемы 8P8C и USB, данные разъемы находятся под крышками, при открытии которых осуществляется блокирование работы и перезапуск аппаратуры. Безопасно открыть данные крышки возможно только в режиме настройки маршрутизатора после прохождения процедуры аутентификации администратора.

4.7 Механизм контроля целостности ключевой информации

Данный механизм позволяет отследить корректность введенной ключевой информации. При вводе ключевой информации с портативного носителя контроль целостности осуществляется следующим образом:

- осуществляется считывание вводимой серии ключей (10 шт.);
- на введенную серию осуществляется расчёт контрольной суммы по алгоритму CRC32 и ее сравнение с эталонной, записанной на портативном носителе;
- серия размаскируется;
- введенная серия ключей разбивается по 1 ключу и на каждый полученный ключ осуществляется расчёт контрольной суммы и ее сравнение с эталонным значением, записанным на портативном носителе, при получении отрицательных результатов контроля целостности хотя бы одного ключа ввод прекращается;

- при получении положительных результатов проверок осуществляется запись ключевой информации в ПЗУ маршрутизатора;
- при получении отрицательных результатов проверок ввод КИ не производится.

После подтверждения целостности всех ключей из вводимой серии осуществляется замаскирование введённой ключевой информации на текущем ключе хранения. Ключ хранения вырабатывается из последнего ключа, принадлежащего текущей ключевой серии – 10-ый порядковый ключ серии отправляется на ПДСЧ для выработки случайной последовательности, после чего осуществляется замаскирование ключей на полученной гамме.

При необходимости смены ключа осуществляется считывание из ПЗУ маршрутизатора замаскированной ключевой информации и расчет контрольной суммы на полученный ключ, затем полученная КС сравнивается с эталонным значением. При получении отрицательных результатов сравнения используется следующий ключ текущей серии, при этом при получении двух подряд ошибок считывания ключевой информации осуществляется блокирование работы маршрутизатора и индикация аварийной ситуации.

Алгоритм работы механизма контроля целостности ключевой информации представлен на рисунке 9.

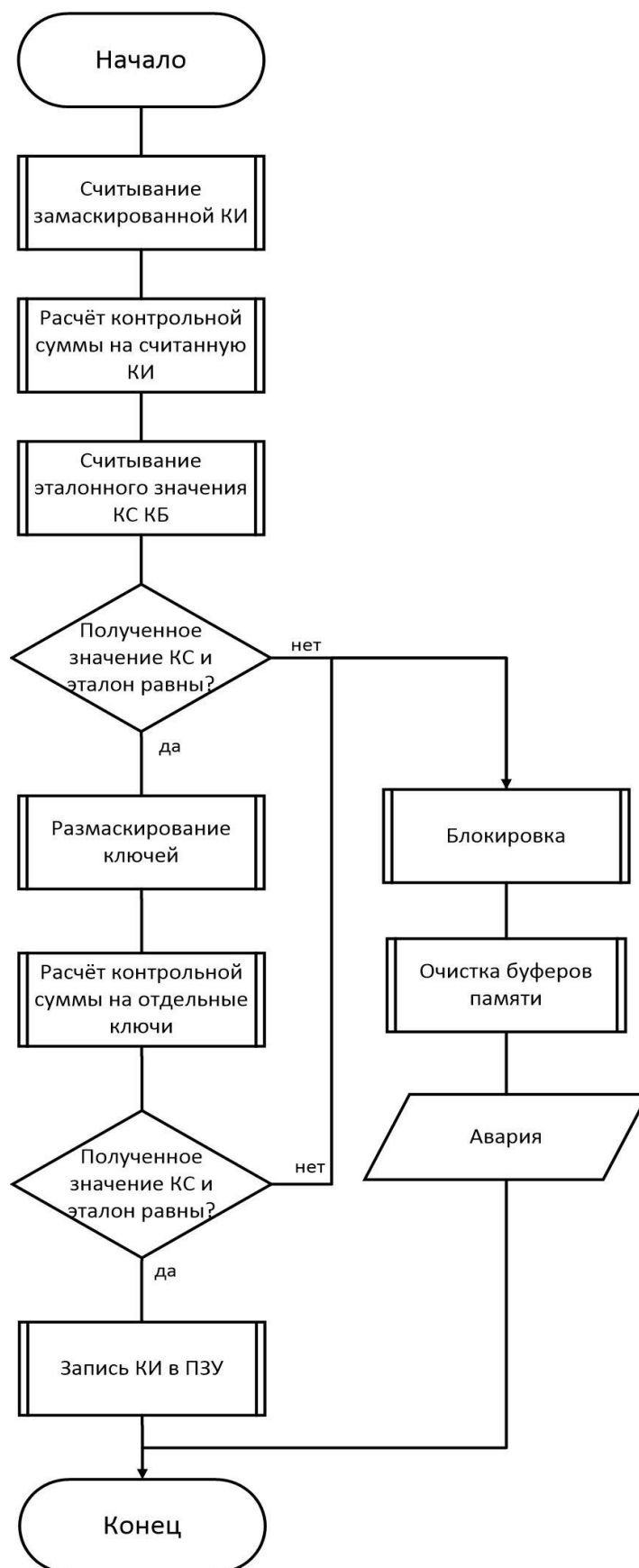


Рисунок 9 – Алгоритм работы механизма контроля целостности ключевой информации

4.8 Алгоритм функционирования контрольно-блокировочных механизмов защиты системы защиты и контроля сетевого трафика

Все вышеизложенные механизмы применяются совместно, при этом алгоритм функционирования представляет собой последовательность применения перечисленных механизмов для достижения наибольшего уровня защищенности системы защиты и контроля сетевого трафика. Применение механизмов осуществляется непрерывно с момента включения питания аппаратуры и до момента его отключения, при этом механизм контроля аккумуляторной батареи осуществляется непрерывно для обеспечения корректной работы механизма защиты от несанкционированного доступа даже в процессе хранения маршрутизатора на складе или транспортировки.

Механизм межсетевого экранирования позволяет анализировать входящий и исходящий трафик в процессе работы, пакеты, не прошедшие проверку, отбрасываются до поступления в коммутационные блоки LAN/WAN.

Алгоритм применения контрольно-блокировочных механизмов представлен на рисунке 10.

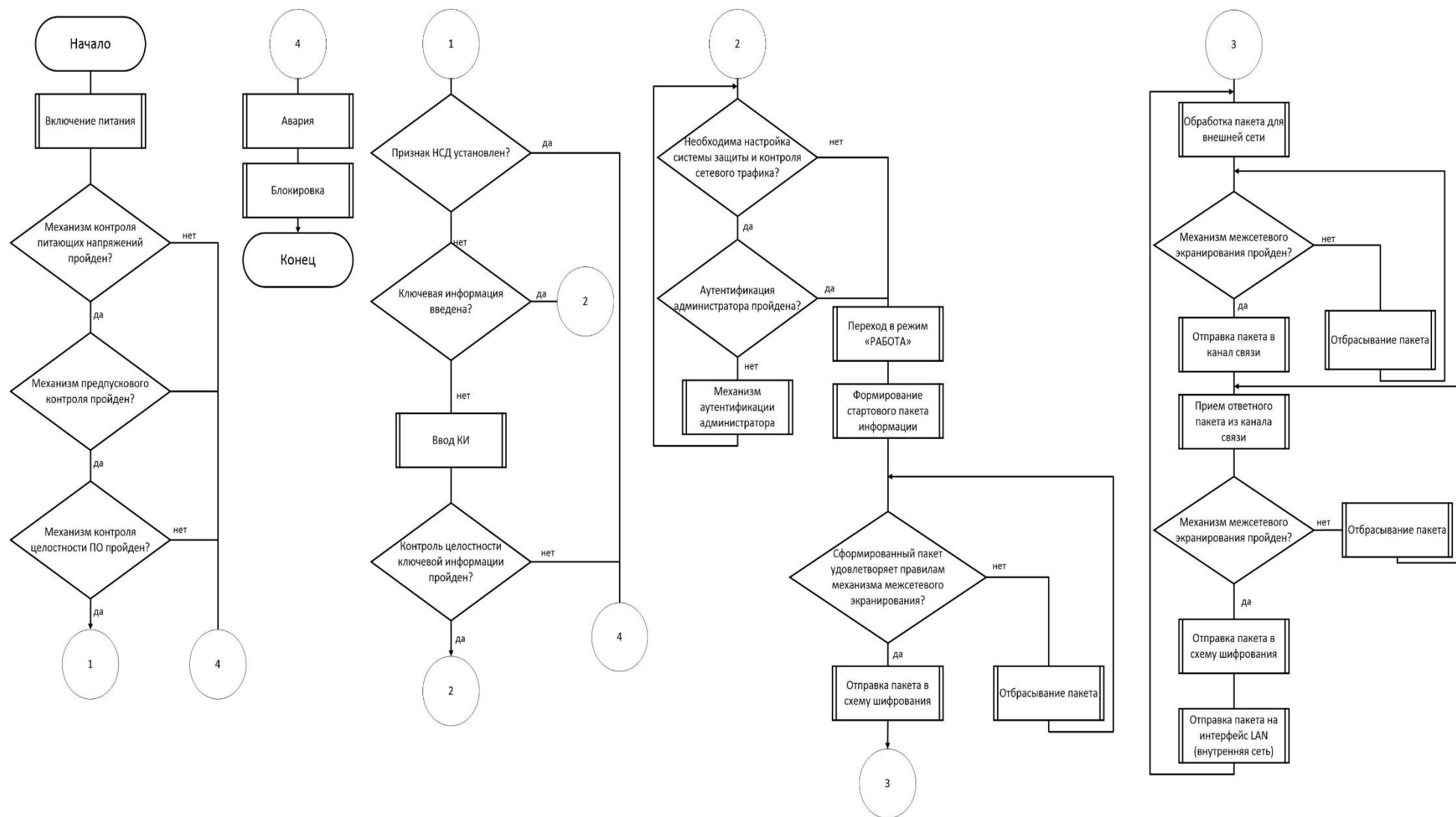


Рисунок 10 – Алгоритм применения и функционирования механизмов защиты и контроля сетевого трафика

4.9 Обоснование отказа от механизмов защиты

При выборе реализуемых механизмов защиты не были выбраны следующие механизмы:

- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрывание внутренней структуры и адресации путем трансляции адресов);
- обнаружение и противодействие атакам (опасным действиям нарушителей).

Отказ от реализации механизма разграничения доступа пользователей обосновывается типом системы – однопользовательская, система имеет только одного пользователя – администратора и после настройки конфигурации функционирует без необходимости вмешательства, за исключением случаев перенастройки. Таким образом, реализацией механизма разграничения доступа является корректность реализации механизма аутентификации в совокупности с организационными мерами защиты и «Руководством администратора».

Изоляцией (защита периметра) компьютерных сетей (фильтрация трафика, скрывание внутренней структуры и адресации путем трансляции адресов) в данном варианте реализации системы защиты и контроля сетевого трафика можно считать реализацию механизма межсетевого экранирования совместно с реализованной криптографической защитой комплекса. Отсутствует необходимость полноценной реализации изоляции компьютерных сетей ввиду избыточности функционала, назначение данного механизма достигается механизмом криптографического закрытия информации – злоумышленник не может получить информацию о структуре сети ввиду наличия зашифрованного трафика.

Отказ от механизма обнаружения и противодействия атакам (опасным действиям нарушителей) обусловлен рядом факторов:

- во внешней сети обмен пакетами осуществляется в криптографически преобразованном виде, соответственно не представляется возможной реализация компьютерных сетевых атак, основанных на ТСР/ІР фрагментации пакетов;
- система защиты и контроля сетевого трафика расположена на территории контролируемой зоны организации, также доступ к СЗИКСТ имеет только администратор данной системы, при отсутствии аутентификации которого аппаратура работает в автоматическом режиме;
- персонал и сотрудники имеют квалификацию в области ИБ, ввиду чего вероятность ошибочных действий со стороны персонала является незначительной.

Исходя из вышеизложенного отсутствует необходимость полноценной реализации механизма обнаружения и противодействия атакам, ввиду выполнения функций данного механизма защиты другими реализуемыми механизмами.

5 Разработка и описание алгоритмов работы, механизмов фильтрации пакетов информации, реализуемых в подсистеме контроля сетевого трафика

5.1 Механизм межсетевого экранирования

5.1.1 Общие положения

Механизм межсетевого экранирования должен обеспечивать фильтрацию входящих и исходящих пакетов информации.

В составе механизма межсетевого экранирования фильтрация пакетов осуществляется по следующим полям:

- механизм фильтрации пакетов по полям «адрес источника» и «адрес получателя»;
- механизм фильтрации пакетов по полям «порт источника» и «порт получателя»;
- механизм фильтрации пакетов по полям «тип протокола».

Механизм фильтрации пакетов по полям «адрес источника» и «адрес получателя» позволяет отследить изменения пакетов данных, которые возникают при попытках реализации атаки подмены сетевых адресов (IP-spoofing). А также позволяют разграничить доступ между подсетями организации (запрет доступа из одной подсети в другую).

Механизм фильтрации пакетов по полям «порт источника» и «порт получателя» позволяет отследить подмену портов источника или получателя, что позволяет исключить возможность перенаправления трафика на скомпрометированный маршрутизатор.

Механизм фильтрации пакетов по полям «тип протокола» позволяет защититься от атак, направленных на сканирование сети, а также избежать ряда проблем, связанных с использованием нестандартных протоколов, набор разрешенных протоколов определяется до внедрения системы защиты и контроля сетевого трафика, при этом маршрутизаторы с реализованной

системой защиты должны находиться в одной сети и иметь непротиворечащие конфигурационные параметры. В качестве основы при проектировании делался упор на протоколы стека TCP/IP ввиду их достаточности для обеспечения сетевого взаимодействия.

Данные механизмы фильтрации при корректной настройке конфигурации системы, в совокупности со схемой шифрования трафика позволяют защититься от большинства сетевых компьютерных атак.

Из наиболее распространенных сетевых компьютерных атак можно выделить:

- атаки, основанные на TCP фрагментации;
- атаки типа IP-spoofing;
- атаки типа ARP-spoofing;
- атаки типа «Man in the middle».

5.1.2 Атаки, основанные на TCP фрагментации

Фрагментация - это коммуникационная процедура, при которой IP-дейтаграмма разбивается на несколько самостоятельных пакетов, которые имеют собственный заголовок и маршрутизируется независимо от других. При потерях фрагментов, по истечении таймаута протоколами более высоких уровней запускается повторная передача дейтаграммы. Фрагментация используется только для пакетов, размер которых превышает заданный Maximum Transmission Unit (MTU) на интерфейсе. MTU — это максимальный объем данных, передаваемый протоколом за одну итерацию, стандартное значение составляет 1500 байт. Этот механизм используется для сокращения времени на повторную передачу в случае возникновения искажения или потери пакета. Уязвимость фрагментации для DDoS-атак заключается в том, что сборка фрагментов осуществляется только в конечном пункте назначения, это позволяет атаковать сервер поддельными пакетами, а также беспрепятственно пройти через роутеры, маршрутизаторы и межсетевые

экраны, т.к. они не пересобирают фрагментированный трафик, и, как следствие, не могут его проанализировать и отбросить как вредоносный.

5.1.3 Атаки типа IP-spoofing

Целью данной атаки является узурпировать IP-адрес определенной машины. Это позволяет злоумышленнику либо скрыть источник атаки (используется в атаках типа "отказ в обслуживании"), либо извлечь какую-либо пользу из доверительных связей двух машин. Атака осуществляется путем подмены информации в пакетах, отправляемых жертве, в качестве обратного адреса IP-адрес хоста (адреса источника) указывается адрес злоумышленника, легко осуществима в UDP, в некоторых случаях возможна в TCP-соединениях.

На сетевом уровне атака частично предотвращается с помощью фильтра пакетов. Он должен быть настроен таким образом, чтобы не пропускать пакеты, пришедшие через те сетевые интерфейсы, откуда они прийти не могли.

5.1.4 Атаки типа ARP-spoofing

ARP-spoofing (ARP — poisoning) — разновидность сетевой атаки типа MITM, применяемая в сетях с использованием протокола ARP. В основном применяется в сетях Ethernet. Атака основана на недостатках протокола ARP.

При использовании в распределённой вычислительной сети алгоритмов удалённого поиска существует возможность осуществления в такой сети типовой удалённой атаки «ложный объект распределённой вычислительной системы». Анализ безопасности протокола ARP показывает, что, перехватив на атакующем узле внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым узлом (например, маршрутизатором), и в дальнейшем активно контролировать

сетевой трафик дезинформированного узла, воздействуя на него по схеме «ложный объект RBC».

Протокол ARP является уязвимым — он не проверяет подлинности ARP-запросов и ARP-ответов. А так как сетевые интерфейсы на компьютерах поддерживают самопроизвольный ARP (ARP-ответ присылается на интерфейс устройства без необходимости), то как раз в таком случае возможна атака ARP-spoofing.

5.1.5 Атаки типа Man in the middle

Man-In-the-Middle (атака посредника, «человек посередине») — вид атаки, когда злоумышленник перехватывает и подменяет сообщения, которыми обмениваются корреспонденты, причем ни один из последних не догадывается о его присутствии в канале. Взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию. Встроившись в коммуникационную цепочку в процессе установления соединения, посредник имитирует вторую сторону коммуникации (как правило, сервер), предоставляя правдоподобно выглядящий сертификат доверия. Чтобы оставаться незамеченным, посредник должен перехватывать все сообщения между клиентом и сервером и зашифровывать, и расшифровывать их соответствующими ключами.

5.1.6 Выбор и обоснование механизмов межсетевого экранирования

Функционирование рассматриваемой корпоративной сети предлагается реализовать на стеке протоколов TCP/IP, что подразумевает, что выход во внешнюю сеть осуществляется с использованием инкапсуляции пакетов данных применяемой при зашифровании трафика и организации криптографически защищенного туннеля с использованием протокола ESP. Ввиду наличия схемы шифрования и полной инкапсуляции пакетов данных злоумышленник может перехватить только зашифрованный пакет данных.

Соответственно для успешной реализации сетевой атаки злоумышленнику необходимо корректно расшифровать полученный пакет, осуществить его модификацию, зашифровать и отправить обратно в канал связи. При попадании на внешний интерфейс системы защиты и контроля сетевого трафика осуществится расшифрование пакета данных с использованием ключевой информации текущей криптографической сессии. Учитывая несоответствие ключевой информации, используемой в текущей криптографической сессии, и КИ, используемой злоумышленником, принятый пакет отбросится еще до попадания на фильтр.

Для защиты сетевого трафика со стороны внутренней сети (внутренний нарушитель) необходимо реализовать средствами межсетевого экранирования фильтрацию пакетов данных по полям:

- адрес источника;
- адрес получателя;
- порт источника;
- порт получателя;
- тип протокола.

Каждый реализованный фильтр должен применяться к любому пакету сети, порядок применения фильтров значения не имеет. При успешном прохождении пакета через все фильтры, он отправляется в схему шифрования и на узел LAN (WAN) маршрутизатора.

Учитывая вышеизложенное, механизм межсетевого экранирования позволяет полностью защититься от сетевых компьютерных атак при условии обеспечения конфиденциальности ключевой информации, используемой криптографической схемой шифрования, и реализации механизма межсетевого экранирования.

Схематичное представление работы механизма межсетевого экранирования представлено на рисунке 11.

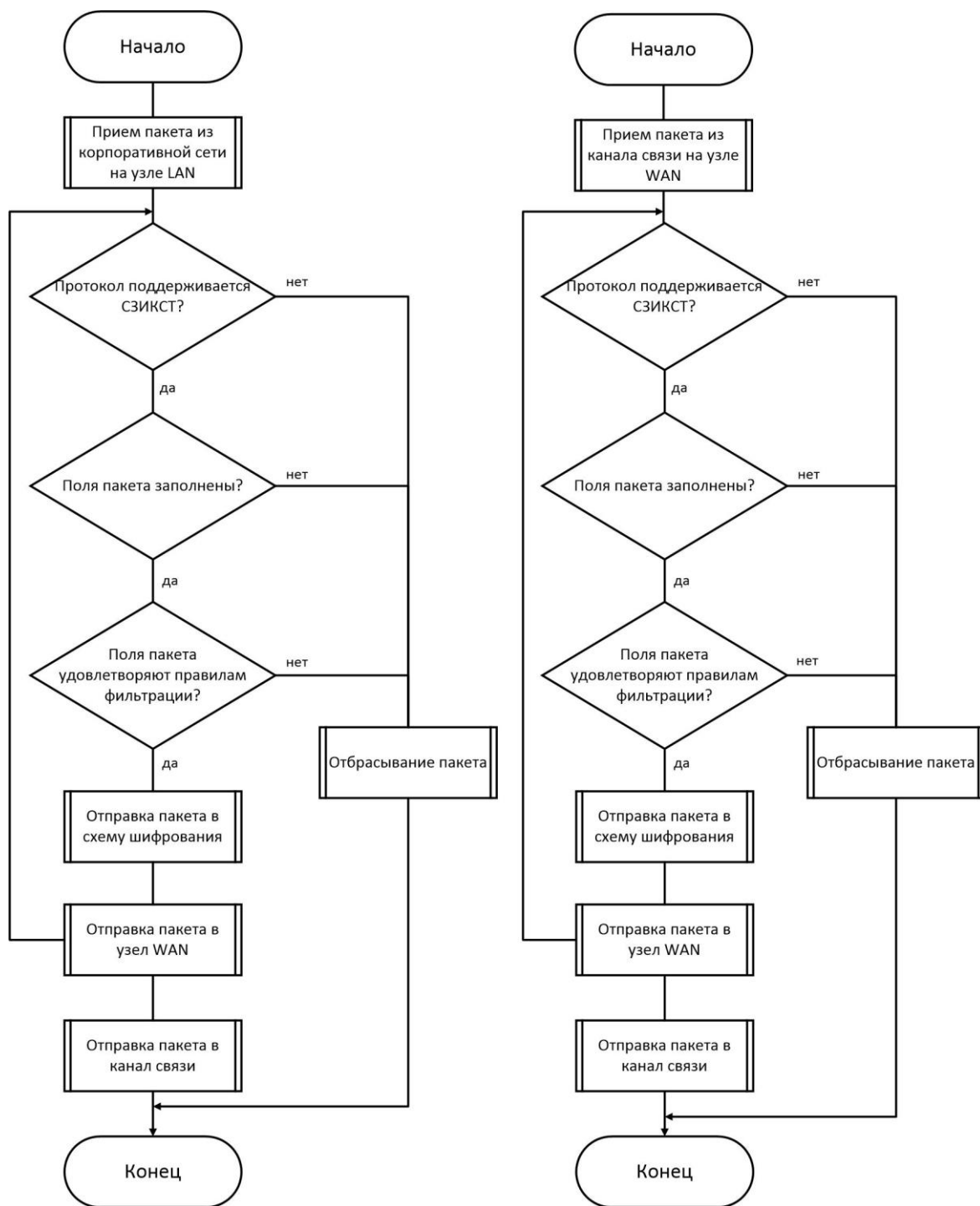


Рисунок 11 – Алгоритм работы механизма контроля сетевого трафика

6 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

6.1 Общие сведения

Так как специалист по защите информации большую часть времени проводит за компьютером, к вредным психофизиологическим факторам, влияющим на нервную систему специалиста по защите информации, можно отнести:

- статическая нагрузка;
- постоянная концентрация внимания;
- большой объем информации, обрабатываемый в единицу времени;
- повышенный уровень электромагнитного излучения.

6.2 Статическая нагрузка

Статическая нагрузка возникает в результате долгосрочного пребывания в статичном состоянии. Статичное состояние – состояние напряжения мышц тела и отсутствие подвижности суставов.

Данное состояние может вызывать застои крови, повышенные нагрузки на поясничный отдел позвоночника, шейный отдел позвоночника. Также данное состояние может возникать в процессе сильной концентрации внимания во время выполнения задания.

Для профилактики возможных заболеваний, сопутствующих статической нагрузке необходимо каждые 2 часа делать перерыв на выполнение комплекса упражнений, направленного на поясничный отдел позвоночника, шейный отдел позвоночника, а также приседания и

скручивания туловища для повышения А/Д, что способствует разгону застойной крови.

6.3 Постоянная концентрация внимания

Работа за компьютером нередко поглощает все внимание работающего человека и потому, такие люди часто пренебрегают нормальным питанием. Неправильное питание приводит не только к нарушениям работы органов пищеварительного тракта, но и к возникновению минеральной и витаминной недостаточности.

6.4 Большой объем информации, обрабатываемый в единицу времени

Работа за компьютером предполагает переработку большого массива информации и постоянную концентрацию внимания, поэтому при длительной работе за компьютером нередко развивается умственная усталость и нарушение внимания, а также это способствует более быстрому наступлению утомления.

Человек, работающий за компьютером, вынужден все время принимать решения, от которых зависит эффективность его работы. Порой бывает довольно сложно предположить последствия того или иного шага. Поэтому, длительная работа за компьютером, часто является причиной хронического стресса. Также необходимость перерабатывать большое количество неоднородной информации может привести к развитию стресса.

6.5 Повышенный уровень электромагнитного излучения

Повышенный уровень электромагнитного излучения от компьютера может привести к повышенной возбудимости нервной системы, проявляющейся раздражительностью, нарушением сна, эмоциональной неустойчивостью. В последующем может развиваться нервно-психическая

слабость. Поэтому при воздействии электромагнитного излучения на организм специалиста по защите информации характерны: головная боль, утомляемость, ухудшение самочувствия. Указанные симптомы могут быть выражены в разной степени.

Предельно допустимая доза электромагнитного излучения для человека составляет 0,2 мкТл. Человек, находясь в непосредственной близости к компьютеру, подвергается электромагнитному излучению, которое в 500 раз превышает допустимое значение. Один из наиболее эффективных способов защиты от негативного воздействия электромагнитного излучения является применение специальных приборов, которые позволяют нейтрализовать данное излучение и максимально минимизировать его негативное воздействие на организм человека. Принцип действия данных приборов основан на наведении противо-ЭДС, которая способствует снижению негативного воздействия на организм человека нежелательных электромагнитных излучений.

При работе за компьютером рекомендуется ставить монитор на расстоянии не ближе 30 см от головы, а также использовать специальные защитные очки для работы с ПК.

Для снижения вреда от психофизиологических факторов, влияющих на нервную систему специалиста по защите информации, следует делать регулярные перерывы в работе. Каждые 30 минут работы за компьютером следует делать, перерыв на 10 минут.

Также следует каждые 2 часа работы выполнять комплекс физических упражнений, предназначенных для малого таза, а также мышц спины и шеи.

Во время перерыва необходимо делать упражнения на расслабление, например, при обнаружении таких симптомов, как сонливость или утомляемость, следует делать следующие упражнения:

- круговые движения головой;
- перевод взгляда с ближнего на дальнее расстояние – одним глазом;

- перевод взгляда с ближнего на дальнее расстояние – двумя глазами.

При обнаружении такого симптома, как головная боль после кропотливой работы, следует делать следующие упражнения:

круговые движения головы; перевод взгляда с ближайших точек на дальние – одним глазом;

- перевод взгляда из угла в угол;
- пальминг;
- общее потягивание тела;
- пожимание плечами, круговые движения плечами.

Вышеперечисленные меры профилактики, меры защиты от вредных факторов должны применяться в системном виде для достижения наиболее качественного результата.

Заключение

В ходе выполнения выпускной квалификационной работы был проведен обзор и анализ существующих релевантных методов защиты информации применяемых в сетях связи. На основании полученных данных были отобраны соответствующие механизмы защиты информации, реализация которых позволяет обеспечить комплексную защиту свойств безопасности информации циркулирующей в сети связи организации. Из полученного перечня механизмов защиты были выбраны только необходимые и достаточные для реализации, обоснованием отказа от остальных механизмов защиты являлось наличие тех же свойств у проще реализуемых.

После определения перечня механизмов защиты информации была разработана структурная схема системы связи организации с применением разрабатываемой системы защиты и контроля сетевого трафика. Учитывая, что сетевая защита реализуется с использованием механизмов криптографического преобразования данных был предложен вариант реализации криптографической схемы соответствующий ГОСТ-28147-89.

Результатом выполнения выпускной квалификационной работы является алгоритм применения выбранных механизмов защиты информации с описанием их алгоритмов функционирования. Каждый механизм из выбранных на предыдущем этапе работы был проанализирован в соответствии с выбранными условиями применения (корпоративная система связи с наличием КЗ и реализованными организационно-техническими мерами защиты информации). Для каждого выбранного механизма защиты были составлены отдельные блок-схемы алгоритмов работы, после чего была составлена общая схема функционирования системы защиты и контроля сетевого трафика, в которой последовательно были расположены все механизмы защиты. Также был предложен алгоритм работы механизма контроля сетевого трафика, представляющий из себя вариант реализации

межсетевого экрана с функциями фильтрации пакетов по содержимому, принадлежащих стеку протоколов TCP/IP.

Исходя из вышеизложенного можно сделать вывод о достижении цели выпускной квалификационной работы. Все пункты технического задания были выполнены в полном объеме. Теоретическая значимость работы заключается в подробном рассмотрении вариантов реализации механизмов защиты информации в сети связи организации и выборе наиболее простого варианта формирования состояния защищенности. Практическая значимость обуславливается в уточнении направления разработки механизмов защиты информации применяемых в совокупности с системами контроля сетевого трафика, а также возможностью применения результатов на предприятиях, соответствующих выбранным условиям применения.

Список используемых источников

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Принят и введен в действие Постановлением Государственного комитета СССР по стандартам от 02.06.89 г. № 1409. – М.: ИПК Издательство стандартов, 1996 - 32 с.
2. Р.В. Мещеряков. Информационная безопасность и защиты информации в сетях ЭВМ: учебное пособие / Р.В. Мещеряков – Томск: изд-во Томского политехнического университета 2008. -147 с.
3. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г: Защита от несанкционированного доступа к информации: Термины и определения - 30 Марта 1992 – 7с.
4. Трансляция сетевых адресов NAT – [Электронный ресурс]. – URL:<http://ciscotips.ru/nat> - Режим доступа: свободный. - (дата обращения 20.05.2020).
5. Защита рабочих станций от несанкционированного доступа при помощи Secret Disk Enterprise – [Электронный ресурс] – URL:https://www.anti-malware.ru/analytics/Technology_Analysis/Secret_Disk_Enterprise - Режим доступа: свободный. – (дата обращения 20.05.2020).
6. Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. Разработаны центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации (ФСБ России). Утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2017 г. N 2068-ст. – М.: Стандартиформ, 2018 - 24с.