ПОРЯДОК ЗАКАЗА, УСТАНОВКИ И ЭКСПЛУАТАЦИИ

Программное обеспечение
«Система однонаправленной передачи данных «INFODIODE»

Содержание

Перечень рисунков

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В тексте документа применены следующие обозначения и сокращения:

АПК	Аппаратно-программный комплекс
ИАФ	Подсистема идентификации, аутентификации и управления доступом
ООО	Общество с ограниченной ответственностью
ОЦЛ	Обеспечение целостности
ПО	Программное обеспечение
РСБ	Регистрация событий безопасности
УПД	Управление правилами доступа
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
FTP	Протокол передачи данных (File Transfer Protocol)
FTPS	Расширение протокола передачи данных FTP, добавлением поддержки для криптографических протоколов уровней транспортной безопасности и защищенных сокетов (File Transfer Protocol + SSL, или FTP/SSL)
INFODIODE	Программное обеспечение «Система однонаправленной передачи данных «INFODIODE»
IP	Маршрутизируемый протокол сетевого уровня стека TCP/IP (Internet Protocol)
NAT	Механизм преобразования IP-адреса транзитных пакетов в сетях TCP/IP (Network Address Translation)
NAT/PAT	Механизм преобразования IP-адреса транзитных пакетов в сетях TCP/IP (Network Address Translation) / и адресного порта (Port Address Translation)
PAT	Трансляция нескольких частных адресов на один или несколько общедоступных адресов (как NAT) с изменением порта (Port Address Translation)
SFTP	Протокол для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения. Протокол разработан как расширение к SSH-2 (SSH File Transfer Protocol)
SIEM	Система сбора информации для анализа и классификации системным администратором или специалистом по ИБ (Security Information and Event Management)
SMB	Сетевой протокол прикладного уровня для межпроцессного взаимодействия, удалённого доступа к файлам, принтерам и другим сетевым ресурсам (Server Message Block)
SMTP	Простой протокол передачи почты (Simple Mail Transfer Protocol)
UDP	Транспортный протокол передачи данных из набора правил TCP/IP для передачи информации (датаграммы) по IP-сети без предварительного установления соединения и создания специального виртуального канала или путей данных (User Datagram Protocol)

Введение

Документ «Порядок заказа, установки и эксплуатации» содержит перечень и краткое описание последовательности действий для приобретения программного обеспечения «Система однонаправленной передачи данных «INFODIODE» (далее ПО, ПО «INFODIODE») в составе аппаратно-программного комплекса (далее АПК).

1 Назначение и автоматизируемые функции

ПО «INFODIODE» - предназначено для установки на серверы, поддерживающие передачу информации по однонаправленной линии связи.

ПО обеспечивает однонаправленную передачу трафика файлов, тегов, UDP, syslog и т.п. из доверенного сегмента за его пределы с возможностью фильтрации отправителей и получателей по IP адресам и портам.

ПО обеспечивает реализацию следующих характеристик АПК:

— скорость передачи – не ниже 300 Mbps при передаче потоковых и пакетных данных;

— передачу потокового UDP трафика с фильтрацией по IP-адресам и портам (выполнение операций NAT/PAT);

— сервис передачи файлов (с разграничением доступа пользователей к сервису) по протоколам FTP, FTPS, SMB, SFTP;

— передачу почтовых сообщений по протоколу SMTP\StartTLS;

— приоритезацию передачи файлов;

— аутентификацию пользователей и групп пользователей сервисов передачи файлов по протоколам FTP, FTPS, SMB, SFTP и почтовых сообщений по протоколу SMTP;

— функциональность коллектора данных (сбор данных на внешнем сервере по протоколам FTP, SMB для целей передачи через аппаратную компоненту).

ПО обеспечивает выполнение следующих требований ФСТЭК России:

— управление (однонаправленная передача) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами (УПД.3);

— разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);

— выполнение функций управления (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1);

— реализацию необходимых методов (ролевой) и правил разграничения доступа (УПД.2);

— идентификацию и аутентификация пользователей, являющихся работниками оператора (ИАФ.1);

— защиту обратной связи при вводе аутентификационной информации (ИАФ.5);

— определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1);

— определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2);

— сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3);

— контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации (ОЦЛ.1).

2 Область применения

ПО в составе АПК предназначено для применения в доверенных сегментах сетей передачи данных для санкционированной передачи за их пределы потоковых данных и файлов.

Организация использования АПК с установленным ПО «INFODIODE» приведена на рисунке 1.

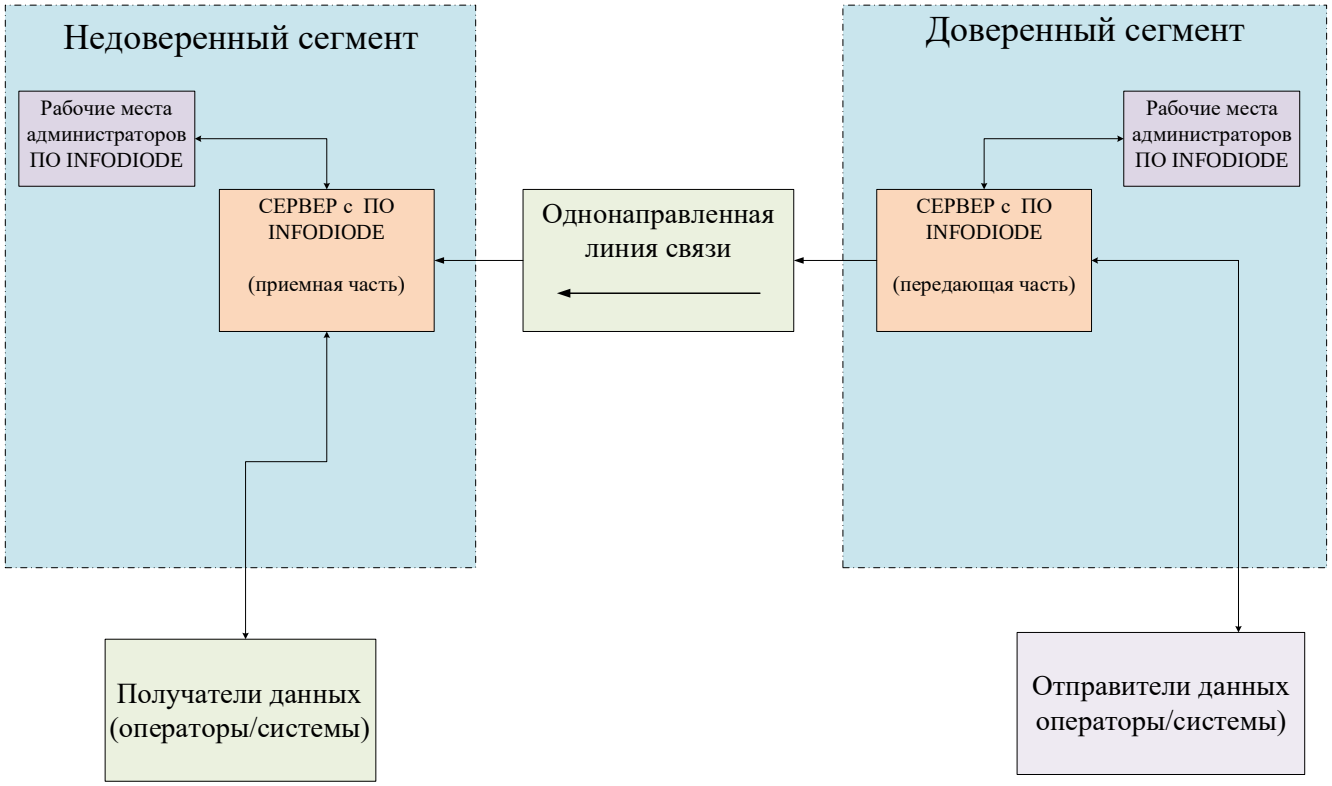

Рисунок 1 — Организация использования АПК

3 Основные функции

Перечисленные ниже функции ПО «INFODIODE» описаны в руководстве оператора, руководстве по эксплуатации и других документах, распространяемых при реализации ПО «INFODIODE».

3.1 Администрирование ПО

Администрирование передающей и приёмной частей ПО «INFODIODE» может быть организовано по нескольким протоколам управления. Подробнее перечень протоколов и особенностей из применения приведены в документе «Руководство по эксплуатации».

Регистрация, удаление и идентификация администраторов в ПО «INFODIODE» реализована с выполнением требований ФСТЭК России.

3.2 Сбор сообщений о регистрируемых событиях

Администраторам предоставлена возможность выбирать значимые события функционирования ПО «INFODIODE», информация о которых должна поступать на указанный адрес syslog коллектора или иных решений по сбору данных, например SIEM.

3.3 Взаимодействие с сетевым оборудованием

ПО «INFODIODE» поддерживает работу взаимодействующего сетевого оборудования имитируя ответы противоположной стороны односторонней лини передачи данных.

3.4 Фильтрация источников и получателей информации

В процессе предварительной настройки ПО «INFODIODE» должны быть указаны в явном виде адреса, порты и протоколы источников и получателей информации. Не указанные в явном виде источники информации игнорируются.

3.5 Функции Proxy сервера

ПО «INFODIODE» обеспечивает реализацию подмены адресов источников и получателей информации.

3.6 Приоритезация трафика

ПО «INFODIODE» позволяет организовать необходимую приоритезацию трафика.

4 Порядок установки и эксплуатации ПО «INFODIODE»

ПО «INFODIODE» распространяется исключительно в составе аппаратно-программных комплексов.

ПО устанавливается представителем ООО «АКТОР ИНФОРМАЦИОННЫЕ СИСТЕМЫ» или представителем организации, с которой у правообладателя ПО установлены договорные отношения на право установки ПО. При установке ПО генерируются лицензионные файлы, учитывающие параметры оборудования и сроки действия лицензии.

ООО «АКТОР ИНФОРМАЦИОННЫЕ СИСТЕМЫ» производит установку ПО на основе договорных отношений. В договоре определяется количество предоставляемых лицензий, их срок действия и ограничения лицензионного соглашения на использование приобретённого ПО.