

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

Программное обеспечение
«Система однонаправленной передачи данных «INFODIODE»

СОДЕРЖАНИЕ

Обозначения и сокращения	3
Введение	4
1 Назначение и автоматизируемые функции	5
1.1 Реализуемые требования ФСТЭК России	5
1.2 Характеристики, реализуемые ПО в составе АПК	5
2 Область применения	7
3 Основные функции.....	8
3.1 Администрирование ПО	8
3.2 Сбор сообщений о регистрируемых событиях.....	8
3.3 Взаимодействие с сетевым оборудованием.....	8
3.4 Фильтрация источников и получателей информации.....	8
3.5 Функции Proxu сервера	8
3.6 Приоритезация трафика	8
4 Характеристика функциональной структуры	9
4.1 Передающая часть	9
4.2 Приемная часть	9
5 Численность, функции и квалификация персонала, эксплуатирующего ПО	10
6 Аппаратные и программные требования для установки ПО	11
6.1 Порядок реализации ПО	11
6.2 Лицензионная поддержка	11
7 Режимы функционирования ПО	12
7.1 Основной режим	12

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 — Организация использования АПК	7
---	---

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В тексте документа применены следующие обозначения и сокращения:

АПК	Аппаратно-программный комплекс
ИАФ	Процедуры обеспечения безопасности информации в части идентификации и аутентификации
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)
SSH	Защищенный протокол удаленного соединения между компьютером-клиентом (домашним компьютером) и компьютером-сервером, позволяющий удаленное управление и передачу данных между ними (Secure SHell)
SSL	Криптографический протокол, использующий асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений (Secure Sockets Layer)
TCP	Протокол управления передачей данных в сети Интернет (Transmission Control Protocol)
TCP/IP	Протокол управления передачей данных/Протокол Интернет (Transmission Control Protocol/Internet 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 «Описание функциональных характеристик» содержит перечень и краткое описание функциональных возможностей программного обеспечения «Система однонаправленной передачи данных «INFODIODE» (далее ПО, ПО «INFODIODE»).

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.

1.1 РЕАЛИЗУЕМЫЕ ТРЕБОВАНИЯ ФСТЭК РОССИИ

ПО разработано для выполнения следующих требований ФСТЭК России:

- управление (однаправленная 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 аутентификацию 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).

1.2 ХАРАКТЕРИСТИКИ, РЕАЛИЗУЕМЫЕ ПО В СОСТАВЕ АПК

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).

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.

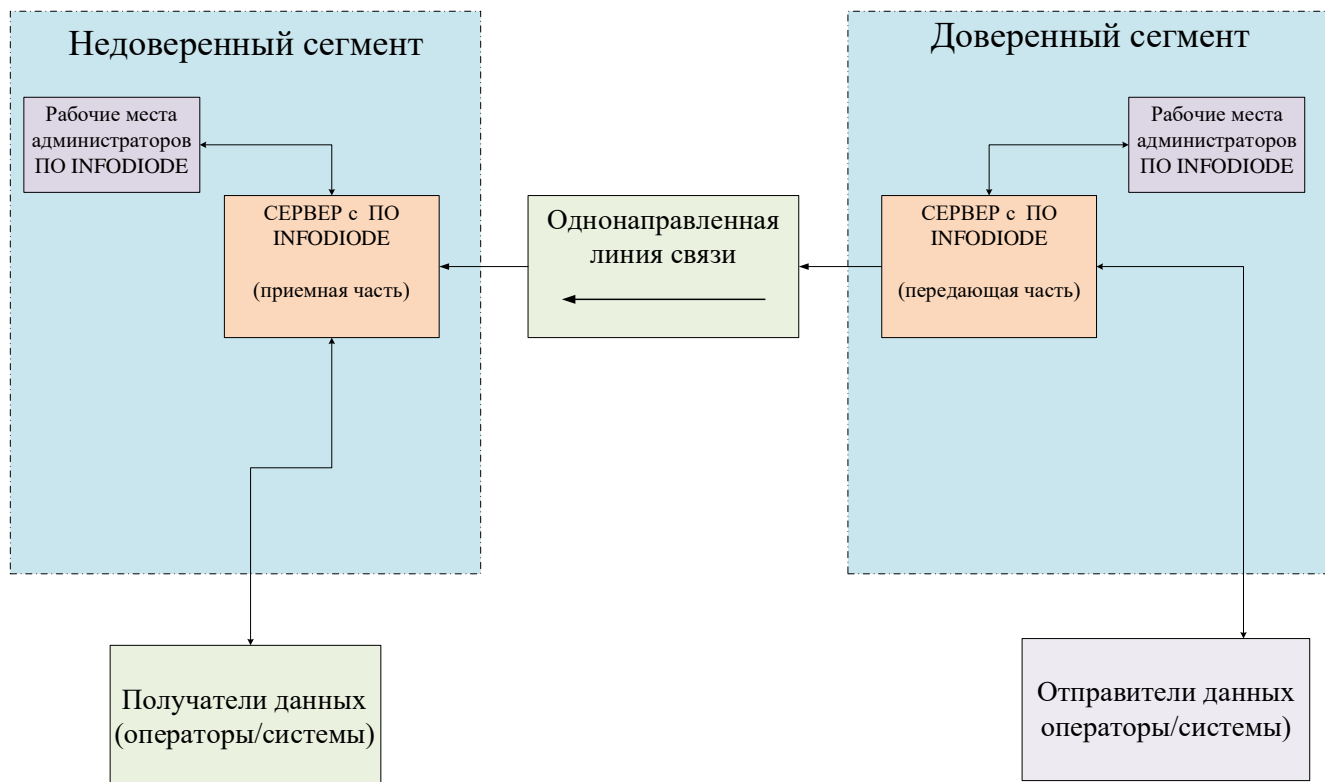


Рисунок 1 — Организация использования АПК

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 линии 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 ХАРАКТЕРИСТИКА ФУНКЦИОНАЛЬНОЙ СТРУКТУРЫ

ПО «INFODIODE» состоит из двух частей – передающей и приемной частей однонаправленной системы передачи информации.

4.1 ПЕРЕДАЮЩАЯ ЧАСТЬ

Передающая часть:

- получает информацию от разрешённых источников информации;
- обеспечивает взаимодействие сетевого уровня с источниками информации и сетевым оборудованием;
- формирует и передает сообщения о регистрируемых событиях;
- поддерживает регистрацию, удаление и доступ администраторов ПО;
- исполняет другие функций, описанные в документации на ПО.

4.2 ПРИЕМНАЯ ЧАСТЬ

Приемная часть:

- отправляет информацию от разрешённых источников информации;
- обеспечивает взаимодействие сетевого уровня с получателями информации и сетевым оборудованием;
- формирует и передает сообщения о регистрируемых событиях;
- поддерживает регистрацию, удаление и доступ администраторов ПО;
- исполняет другие функций, описанные в документации на ПО.

5 ЧИСЛЕННОСТЬ, ФУНКЦИИ И КВАЛИФИКАЦИЯ ПЕРСОНАЛА, ЭКСПЛУАТИРУЮЩЕГО ПО

ПО «INFODIODE» может обслуживаться администратором сетевой инфраструктуры доверенного сегмента и администратором сетевой инфраструктуры узла получения данных. См. рисунок 1.

6 АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ ДЛЯ УСТАНОВКИ ПО

6.1 ПОРЯДОК РЕАЛИЗАЦИИ ПО

ПО «INFODIODE» реализуется в составе АПК и требования к аппаратному обеспечению (серверам) согласуются на этапе организации продажи на договорной основе.

6.2 ЛИЦЕНЗИОННАЯ ПОДДЕРЖКА

Реализуемое ПО «INFODIODE» лицензируется с привязкой к серверному оборудованию. При замене вышедших из строя серверов заменяется лицензия на ПО.

Порядок замены лицензии при отказе оборудования и продлении эксплуатации ПО определяется на договорной основе при приобретении ПО.

7 РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ ПО

7.1 ОСНОВНОЙ РЕЖИМ

ПО обеспечивает:

- непрерывную работу в режиме – 24 часа в день, 7 дней в неделю (24x7);
- выполнение всех функций в полном объеме; за исключением периодов проведения профилактических и других работ, а также устранения возникших нештатных ситуаций.