АО «Концерн «Автоматика»

УТВЕРЖДЕН
УВИР.30500.001 31 01-ЛУ

СИСТЕМА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК «ФОРПОСТ»

Версия 3.0
Исполнение 4

Описание применения
Версия для работы под ОС Linux

УВИР.30500.001 31 01

Листов 26

2022

АННОТАЦИЯ

Настоящий документ содержит описание применения сертифицированной версии программного комплекса системы обнаружения компьютерных атак СОА «Форпост» версии 3.0 исполнение 4. В документе описываются назначение и функциональность системы, ее характеристики, системные требования, особенности применения. Так же приведены описание логической структуры, требования к окружению, в котором должна функционировать система, типовая схема включения в автоматизированную информационную систему (АИС).

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и функциональность продукта

1.1.1 Программный комплекс система обнаружения компьютерных атак «Форпост» версия 3.0 исп. 4 (в дальнейшем – СОА «Форпост» или система), предназначена для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему (в дальнейшем – АИС), которые могут быть классифицированы как компьютерные атаки или вторжения, блокирования развития выявленных компьютерных атак, отслеживания состояния контролируемых ресурсов автоматизированной информационной системы и разбора ситуаций в случае возникновения проблем с доступностью к ИТ-сервисам. СОА «Форпост» представляет собой многокомпонентную распределенную систему обнаружения компьютерных атак, применяемую для защиты информации, обрабатываемой в:

– государственных информационных системах;

– критических информационных системах;

– системах, обрабатывающих персональные данные;

– прочих автоматизированных информационных системах, как компонент подсистемы защиты информации от несанкционированного доступа.

1.1.2 ПК СОА «Форпост» реализует возможность:

– построения как небольших, так и территориально распределённых иерархических СОА, дополнительно обеспечивающих мониторинг и управление комплексом технических средств защищаемой информационной системы (далее ИС);

– выявление компьютерных атак и компьютерных инцидентов;

– интеграцию с внешними системами:

- системами оперативной поддержки принятия решений;
- SIEM;
- ГосСОПКА.

1.1.3 Система обеспечивает:

– обнаружение компьютерных атак, направленных на серверы телематических служб (WEB, FTP, электронная почта, СУБД) и рабочие станции, размещенные в контролируемых сегментах;

– предотвращение развития сетевых компьютерных атак путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору,

маршрутизатору), по протоколам RS-232, CLI, telnet, SSH, соответствующей последовательности команд на основе шаблонов (при Т-образном подключении сетевого датчика);

– блокирование трафика, содержащего элемент компьютерной атаки (при U-образном подключении сетевого датчика Linux-версии);

– контроль нормального функционирование комплекса технических средств (далее КТС) защищаемой системы и объектов;

– контроль неизменности прошивок и управляющей информации сетевого оборудования;

– контроль неизменности состава и версионности программного обеспечения на рабочих станциях и серверах информационной системы и объектовых систем управления;

– контроль и ведение журнала сообщений операционной системы на АРМах и серверах информационной системы;

– контроль и ведение журнала сообщений прикладного и специального ПО на рабочих станциях и серверах информационной системы;

– контроль доступности узлов локальной сети, защищаемой ИС и неизменность используемых в данной ЛВС сетевых протоколов и их портов;

– оповещение администратора СОА об обнаруженных атаках, зафиксированных изменениях в работоспособности и настройках КТС и программного обеспечения, размещённого в/на них путем вывода соответствующего сообщения на консоль администратора СОА, записи сообщения в специальный журнал, путем отправки сообщений по электронной почте;

– контроль целостности собственных ресурсов СОА и ресурсов защищаемой АИС, а также, за счет этого механизма, возможность отслеживания действий нарушителей по отношению к контролируемым ресурсам в скомпрометированной системе;

– ведение журнала системных сообщений, содержащего служебную информацию, формируемую компонентами СОА, журнала сообщений от сетевого оборудования, поступающих по протоколам SNMP и syslog;

– интеграцию с внешними системами путем передачи сообщений о зафиксированных компьютерных атаках из журнала СОА по протоколу syslog;

– генерацию отчетов на основе содержимого журналов СОА;

– отслеживание появления новых сообщений системных журналов;

1.1.4 Продукт обладает подсистемой собственной безопасности, которая позволяет шифровать передаваемую между территориально распределёнными компонентами информацию с использованием отечественных СКЗИ, осуществлять контроль целостности собственных ресурсов и ресурсов защищаемой АИС.

1.1.5 ПК СОА «Форпост» иметь возможность использования на технических средствах с архитектурой X86 и «Эльбрус», работающих под управлением ОС:

– семейства Windows (только узловой датчик);
– Linux, семейства Debian;
– Astra Linux, включая исполнение «SE»: «Смоленск», «Ленинград»;

1.1.6 Поддерживаемые среды виртуализации:

– VMware ESXi;
– Kernel-based Virtual Machine (KVM);
– Microsoft Hyper-V.

1.2 Описание логической структуры системы

СОА «Форпост» имеет распределенную многомодульную архитектуру (логическая структура СОА «Форпост» представлена на рисунке 1.2.1).

Модули могут быть установлены как на один сервер, так и распределены на несколько в зависимости от требуемых показателей производительности и отказоустойчивости.

1.2.1 Между компонентами ПК СОА «Форпост» (в случае использования как распределённой СОА) при информационном обмене используется протокол TLS. При этом для защиты передаваемой информации, и аутентификации компонент могу применяться отечественные сертифицированные СКЗИ «КриптоПро CSP» версии 4.0 и 5.0.

В качестве хранилища данных СОА «Форпост» использует СУБД PostgreSQL, которая устанавливается на узел, где расположен компонент «Форпост Сервер».

1.2.2 **Компонент «Форпост Сервер»**, в сертифицированном исполнении, работает под ОС Linux и является связующим звеном между модулями системы: обеспечивает передачу информации между ними, выполняет функции контроля работоспособности компонентов.

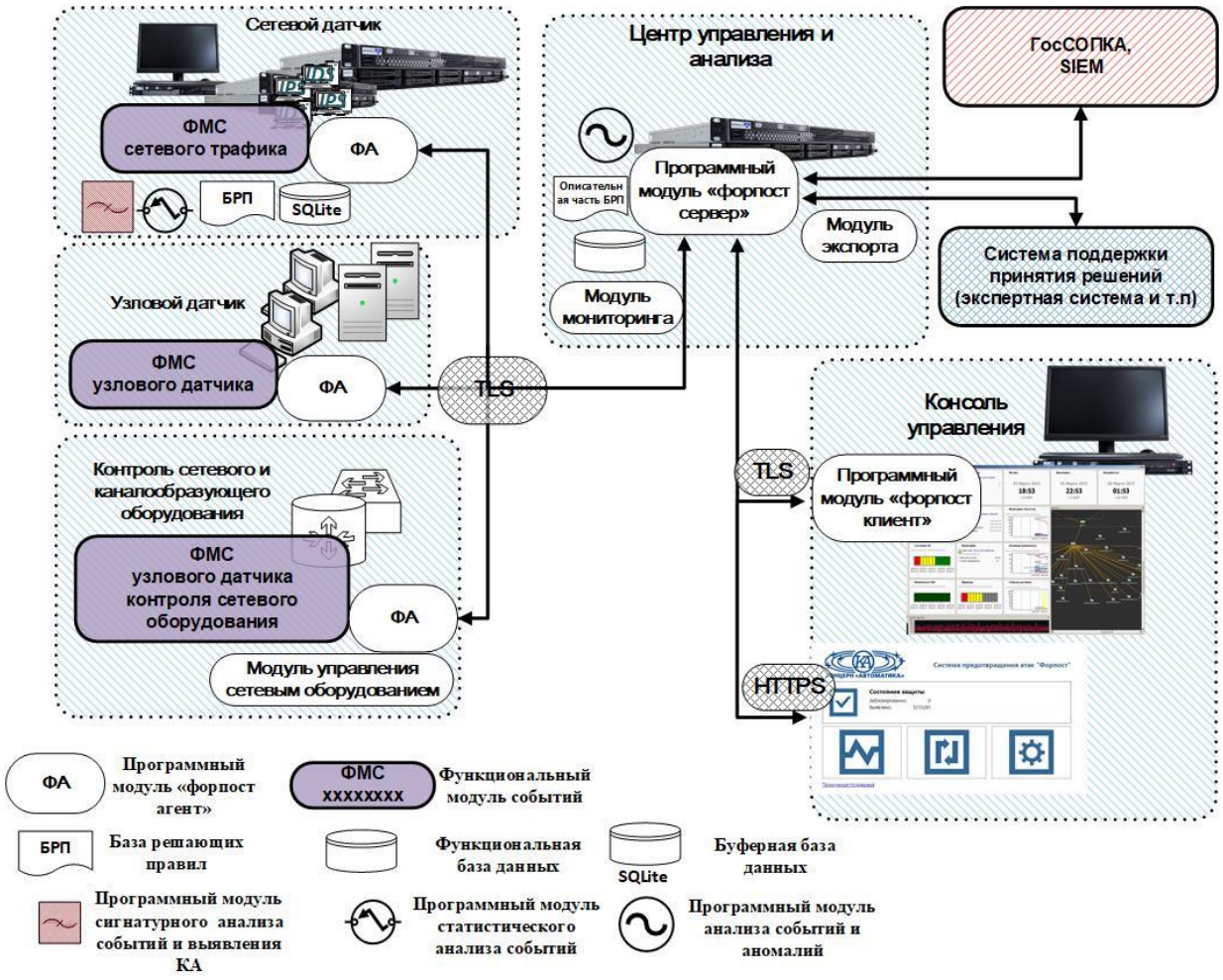

Рисунок 1.2.1 – Логическая структура СОА «Форпост».

1.2.3 Компонент «К**онсоль управления**» реализован в 2-х вариантах:

– консоль управления с использованием «толстого клиента» Компонент «Форпост Клиент» для распределённых и больших систем;

– Web консоль для единичных ПАКов IDS/IPS для упрощённого оперативного управления.

1.2.4 Компонент «**Форпост Клиент**» (консоль администратора) работает под управлением ОС Windows или Linux, обеспечивает графический русскоязычный и англоязычный пользовательский интерфейс, позволяющий:

– просматривать текущее состояние компонентов системы;

– производить удаленную установку, настройку и удаление компонентов системы, для которых предусмотрена такая возможность;

– просматривать информацию об обнаруженных атаках и нарушении целостности файлов в соответствующем журнале;

– просматривать системные сообщения, генерируемые компонентами СОА в журнале системных сообщений;

– просматривать в журнале сетевого оборудования сообщения от подключенного к СОА сетевого оборудования;

– просматривать системный журнал, содержащий служебную информацию, формируемую компонентами СОА и информацию об управлении подключенным сетевым оборудованием;

– производить настройку модулей системы;

– производить блокировку источника атаки с помощью сетевого оборудования;

– управлять подключенным к СОА сетевым оборудованием (межсетевые экраны, коммутаторы, маршрутизаторы и т. д.);

– производить выборку ранее произошедших событий с использованием гибкой системы фильтрации;

– генерировать отчёты на основе содержимого журналов СОА.

1.2.5 Компонент «**Форпост Агент**» (работает под управлением ОС Linux) выполняет функции управления датчиками или модулями системы, а также функции обеспечения передачи информации между датчиками и компонентом «Форпост Сервер».

Дополнительно в компонент «Форпост Агент» пользователем системы может быть встроен «**Модуль удаленного управления**», предоставляющий доступ к рабочему столу удаленного узла под управлением ОС «Windows».

1.2.6 Компонент **«Сетевой датчик**» осуществляет анализ поступающего трафика на наличие в нем компьютерных атак используя сигнатурный метод. Сетевой датчик, работающий под управлением ОС «Windows», поддерживает Т-образный способ подключения (к зеркалирующему (SPAN) порту коммутатора, межсетевого экрана, специализированного ответвителя трафика (TAP) и пр.). Сетевой датчик, работающий под управлением ОС «Linux», поддерживает как Т-образный способ подключения, так и U-образный («в разрыв» на границе защищаемого сегмента).

1.2.7 Компонент «**Узловой датчик**» (работает под управлением ОС Windows или Linux) собирает следующую информацию с узлов, на которых он установлен:

– информация о доступности узла;

– информация о типе процессора, памяти, жестких дисков и пр., а также информация об их загрузке;

– информация об установленном ПО;

– информация из системных журналов ОС;

– прочая служебная информация.

1.2.8 Компонент **«Датчик контроля целостности»** (работает как под управлением ОС Windows, так и Linux) производит контроль целостности собственных ресурсов СОА и ресурсов защищаемой АИС:

– исполняемых файлов;

– конфигурационных файлов;

– веток реестра;

– файлов, периодически загружаемых для контроля по протоколу tftp.

В своей работе указанный компонент использует СКЗИ КриптоПро CSP.

1.2.9 Компонент **«Модуль мониторинга»** (работает под управлением ОС Windows или Linux) контролирует:

– доступность удаленных узлов с помощью отправки ICMP-запросов (Ping);

– доступность сервисов, ожидающих подключение по протоколу TCP, с помощью операции установки TCP-соединения с указанным сервисом;

Дополнительно в указанный компонент встроен сканер TCP/UDP-портов.

1.2.10 Компонент **«Модуль управления сетевым оборудованием»** выполняет следующие функции:

– предоставляет возможность посылать команды сетевому оборудованию (коммутаторам, межсетевым экранам и др.) напрямую, либо, на основе шаблонов по протоколам RS-232, telnet, SSH, например, с целью блокирования компьютерной атаки в стадии ее развития.

– предоставляет возможность приема SNMP и syslog-сообщений от различных узлов сети (коммутаторы, межсетевые экраны и др.) с последующей их обработкой и выводом в журнал СОА в понятном для пользователя виде.

1.2.11 Компонент **«Модуль экспорта»** выполняет следующие функции:

– предоставляет возможность экспорта сообщений, поступающих в журнал СОА, в различные внешние системы корреляции и мониторинга (такие как Cisco Mars, ArcSight, Maxpatrol SIEM, «КОМРАД» и др.) по протоколу syslog;

– отправка по электронной почте (по протоколу SMTP) заранее заданным адресатам информации об обнаруженных атаках и событиях, происходящих в системе.

1.3 Системные требования

1.3.1 СОА «Форпост» версии 3.0 работает под управлением следующих операционных систем:

- Astra Linux Special Edition 1.7 (релиз «Смоленск»);
- специального назначения Astra Linux Special Edition (исполнение РУСБ.10265-01).

на русском и английском языках.

Необходимо, чтобы ОС была настроена в соответствии с политикой безопасности, предполагающей, в частности, контроль (разграничение) доступа и запуск монитора обращений до запуска собственно СОА. Таким образом должна быть обеспечена невозможность внесения модификаций недоверенными субъектами.

1.3.2 При первоначальном запуске, периодически во время нормального функционирования, а также по запросу администратора должен выполняться пакет тестовых программ для демонстрации правильности выполнения предположений безопасности. В частности, необходима проверка возможности доступа СОА «Форпост» ко всем объектам контролируемой информационной системы, а также синхронизации по времени как между компонентами СОА, так и между СОА и информационной системой (например, операционной системой, на которой функционируют компоненты).

1.3.3 Система является распределенной, поэтому компоненты системы могут быть установлены как на нескольких узлах, так и на одном. На каждом узле может быть разная операционная система.

1.3.4 СОА «Форпост» версии 3.0. работает совместно со следующими СУБД:

- PostgreSQL версия 9;
- PostgreSQL версия 10;

на русском и английском языках.

На доступ к БД должен быть установлен пароль для предотвращения несанкционированного удаления или модификации записей аудита. Также СУБД необходимо настроить так, чтобы она сигнализировала о переполнении журнала (либо окончании свободного места на диске/дисках).

1.3.5 СОА «Форпост» версии 3.0. поддерживает среды виртуализации:

- VMware ESXi
- Kernel-based Virtual Machine (KVM)
- Microsoft Hyper-V

1.3.6 Минимальные системные требования:

- процессор с частотой не менее 1,6 ГГц;

– оперативная память выбирается исходя из числа потоков процессора. На 1 поток необходимо 2 Гб оперативной памяти;

– объем свободного дискового пространства не менее 20 ГБ;

– сетевой интерфейс со скоростью не менее 100 Мбит/с;

– на узле с сетевым датчиком в режиме IDS – дополнительно не менее 1 сетевого интерфейса для захвата трафика со скоростью не менее 100 Мбит/с предпочтительно в серверном исполнении;

– на узле с сетевым датчиком в режиме IPS – дополнительно не менее 2 сетевых интерфейсов для захвата трафика со скоростью не менее 100 Мбит/с предпочтительно в серверном исполнении.

1.3.7 При повышенных требованиях по производительности рекомендуется:

− на серверах с компонентами «Форпост Сервер» и «Сетевой датчик» увеличить тактовую частоту процессора и использовать многоядерные, либо многопроцессорные конфигурации; использовать серверные версии операционной системы;

− привести объем дискового пространства в соответствие с потребностями СУБД по объему единовременно хранимой в системе информации о событиях;

− на серверах с компонентом «Сетевой датчик» для захвата трафика использовать сетевые интерфейсы со скоростью 1 Гбит/с в серверном исполнении.

− для обработки сетевым датчиком потока трафика со скоростью 1 Гбит/с, число процессорных ядер должно быть не менее 8 шт. Для обработки трафика со скоростью 500 Мбит/с, число процессорных ядер должно быть не менее 4 шт.

1.4 Реализуемые функции безопасности

1.4.1 В Изделии реализованы следующие функции безопасности:

− разграничение доступа к управлению СОВ, идентификация и аутентификация;

− управление работой СОВ;

− управление параметрами СОВ;

− управление установкой обновлений (актуализации) БРП СОВ;

− анализ данных СОВ;

− аудит безопасности СОВ;

− сбор данных о событиях и активности в контролируемой ИС;

− реагирование СОВ;

− контроль целостности компонентов СОВ, ПО сетевого оборудования и ПО объектовых систем управления.

Сопоставление функций безопасности, реализуемых ОО и мер защиты согласно Приказов ФСТЭК России № 17 от 11.02.2013, № 21 от 18.02.2013, № 31 от 14.03.2014 и № 239 от 25.12.2017 приведено в таблице 2.

Таблица 1 – Сопоставление функций безопасности, реализуемых СОА «Форпост» версии 3.0 исполнение 4 и мер защиты

Функции безопасности	Функции безопасности ОО в соответствии с ЗБ	Условное обозначение меры защиты	Примечание
Разграничение доступа к управлению СОВ, идентификация и аутентификация	FAU_GEN.2 FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.2 FIA_UID.2 FMT_SMR.1 FID_CON_EXT.1 FID_INF_EXT.1	ИАФ.1 ИАФ.2 ИАФ.3 ИАФ.5 УПД.1 УПД.2 УПД.6 УПД.4 УПД.10	Реализуется в отношении пользователей СОВ
Управление работой СОВ	FMT_MOF.1 FID_INF_EXT.1	СОВ.1 СОВ.2	
Управление параметрами СОВ	FMT_MOF.1 FMT_MTD.1 FMT_MTD.2	ОПС.1 ОПС.2	
Управление установкой обновлений (актуализации) БРП СОВ	FID_UPD_EXT.1	СОВ.2	
Анализ данных СОВ	FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FID_ANL_EXT.1	РСБ.1 РСБ.2	
Аудит безопасности СОВ	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1	РСБ.1 РСБ.2 РСБ.3	

Функции безопасности	Функции безопасности ОО в соответствии с ЗБ	Условное обозначение меры защиты	Примечание
	FAU_SAR.2 FAU_SAR.3 FPT_TST.1 FID_COL_EXT.1 FID_ANL_EXT.1 FID_RCT_EXT.1	РСБ.4 РСБ.6	
Сбор данных о событиях и активности в контролируемой ИС	FID_COL_EXT.1 FID_MTH_EXT.1 FID_MTH_EXT.2 FID_PCL_EXT.1	РСБ.1 РСБ.3	Реализуется в отношении ИС
Реагирование СОВ	FMT_MOF.1 FMT_MTD.1 FMT_MTD.2 FMT_SMR.1 FID_COL_EXT.1 FID_ANL_EXT.1 FID_MTH_EXT.1 FID_RCT_EXT.1 FID_PCL_EXT.1 FID_CON_EXT.1 FID_UPD_EXT.1 FID_INF_EXT.1	УПД.2 УПД.4 РСБ.5 АНЗ.1 АНЗ.2	Реализуется в отношении ИС
Контроль целостности компонентов СОВ, ПО сетевого оборудования и ПО объектовых систем управления	FPT_TST.1	ОЦЛ.1	

1.5 Особенности применения продукта

1.5.1 СОА «Форпост» имеет следующие особенности применения:

− уведомление администратора о возникновении ситуации, требующей его внимания через графическую консоль администратора и по электронной почте;

− хранение всей накопленной системой информации на протяжении достаточно длительных периодов может приводить к уменьшению производительности, что связано с большими объемами данных, обрабатываемых системой, поэтому в ходе эксплуатации СОА «Форпост» необходимо производить периодическое удаление несущественной информации;

1.5.2 СОА «Форпост» предъявляет высокие требования к квалификации и компетентности эксплуатирующего персонала, связанные со спецификой предметной области.

2 ОПИСАНИЕ УСЛОВИЙ ПРИМЕНЕНИЯ

2.1 Требования к окружению

2.1.1 Для работы информационного фонда СОА «Форпост» на серверах, предназначенных для его установки, должна быть развернута система управления базами данных (СУБД) согласно системным требованиям продукта.

2.1.2 Для использования в подсистеме собственной безопасности СОА «Форпост» отечественных криптоалгоритмов, на все узлы, на которые установлены компоненты СОА «Форпост», требуется установка внешнего крипропровайдера. В настоящее время поддерживается работа со средством криптографической защиты информации (СКЗИ) КриптоПро CSP 4.0.

2.1.3 Для обеспечения криптографически защищенного (шифрованного) информационного обмена между компонентами СОА «Форпост», а также для обеспечения работы функции контроля целостности ресурсов, требуется доступ к услугам удостоверяющего центра.

2.1.4 Для обеспечения нормальных условий функционирования и исключения возможности вмешательства в работу СОА нарушителей информационной безопасности рекомендуется:

– Использование криптографически защищенного информационного обмена между компонентами СОА, настроенного согласно инструкциям, изложенным в эксплуатационной документации СОА.

– В случае, если обеспечить криптографическую защиту информационного обмена по тем или иным причинам невозможно, компоненты СОА должны устанавливаться в выделенном сетевом сегменте, защищаемом от воздействия нарушителя организационно-техническими мерами.

– Доступ к программно-аппаратным средствам, на которых установлены и функционируют компоненты СОА, (в том числе файлам настроек и исполняемым файлам) должен предоставляться только уполномоченным доверенным пользователям, не являющимся нарушителями информационной безопасности.

– В случае, если пользователи, имеющие доступ к программно-аппаратным средствам, на которых установлены и функционируют компонентам СОА, могут являться нарушителями, контроль за действиями пользователей должен обеспечиваться соответствующими организационно-техническими мерами.

– Управление сетевым оборудованием, блокировка источников компьютерных атак, а также получение информации о состоянии сетевого оборудования должно производиться через выделенное (изолированное от нарушителя) подключение к отдельным сетевым портам указанного сетевого оборудования.

2.2 Типовая схема включения СОА «Форпост»

2.2.1 Подключение СОА «Форпост» к защищаемой АИС, в режиме сетевой СОА, зависит от режима сетевого датчика:

- IDS – система обнаружения вторжений;
- IPS – система предотвращения вторжений.

2.2.2 Сетевой датчик в режиме IDS устанавливается на зеркалирующий порт коммутатора (SPAN порт).

2.2.3 Сетевой датчик в режиме IPS необходимо ставить «в разрыв» между предполагаемым нарушителем и защищаемым сегментом.

2.2.4 Типовая схема включения СОА «Форпост» с сетевым датчиком в режиме IDS в АИС представлена на рисунке 2.2.1.

2.2.5 Типовая схема включения СОА «Форпост» с сетевым датчиком в режиме IPS в АИС представлена на рисунке 2.2.2.

2.2.6 Предполагается, что защищается сегмент пользователей.

2.2.7 На каждый АРМ пользователя устанавливаются следующие компоненты:

- «Хостовой датчик» для контроля и мониторинга состояния АРМ;
- «Форпост Агент» для связи с компонентом «Форпост Сервер» (на ОС Linux устанавливается совместно с хостовым датчиком);
- «Датчик контроля целостности» для контроля целостности файлов на АРМ (на ОС Linux устанавливается совместно с хостовым датчиком).

2.2.8 В приведенных схемах компоненты «Сетевой датчик», «Форпост Сервер», «Форпост Клиент», «Модуль монитора», «Модуль управления сетевым оборудованием» и СУБД распределены на несколько серверов, так же эти компоненты могут быть установлены на один сервер.

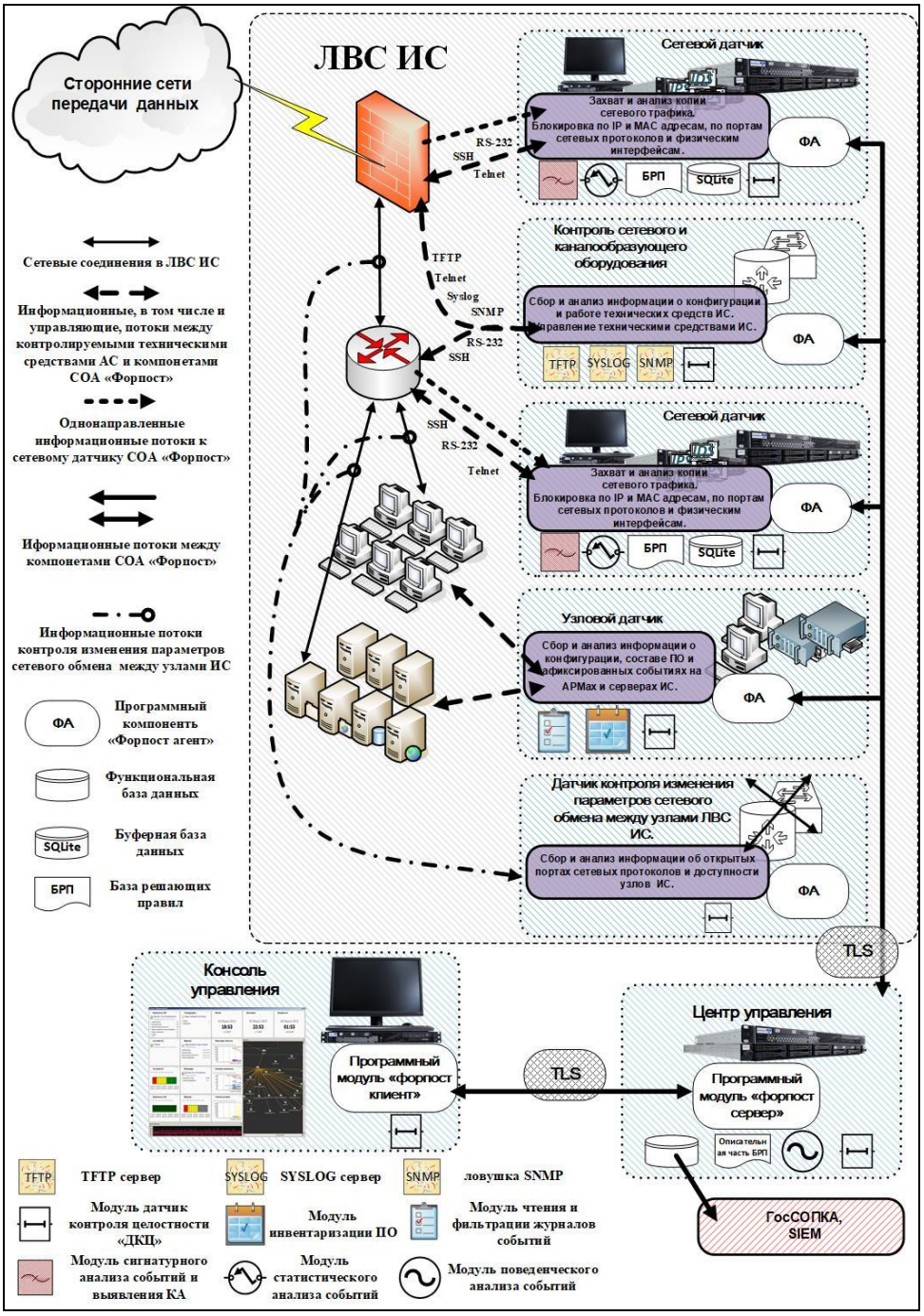

Рисунок 2.2.1 – Типовая схема включения СОА «Форпост» при Т-образном способе подключения сетевого датчика

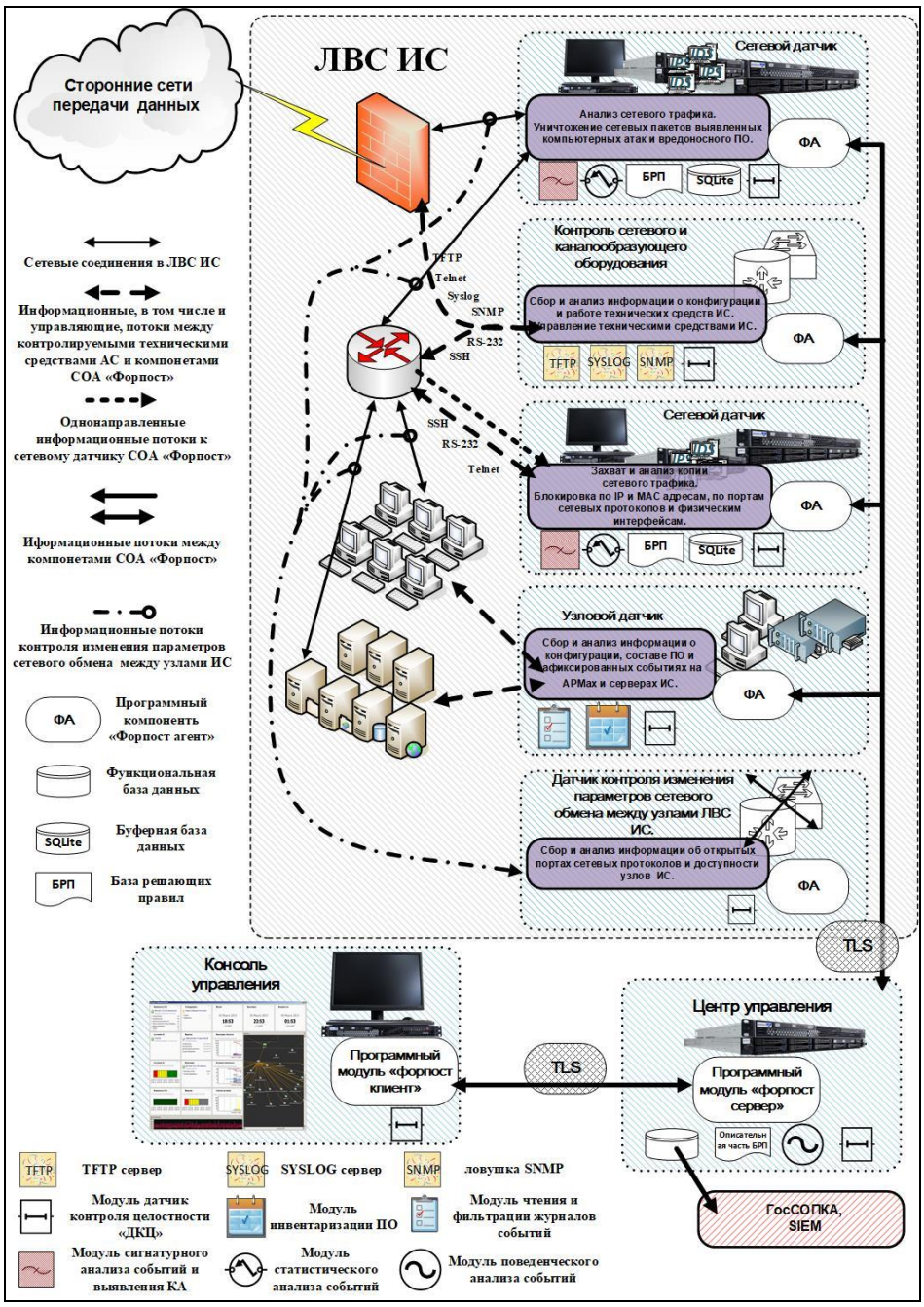

Рисунок 2.2.2 – Типовая схема включения СОА «Форпост» при U-образном способе подключения сетевого датчика

2.2.9 В качестве точки включения в АИС для сетевого датчика в режиме IDS могут выступать:

− зеркалирующий порт коммутатора (SPAN-порт), коммутатор при этом настраивается таким образом, чтобы пакеты, поступающие на его порты, копировались в зеркалирующий порт;

− контролирующий порт специализированного агрегирующего ответвителя трафика, который устанавливается «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика;

− порт сетевого концентратора (hub), который может быть установлен вместо коммутатора, либо «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика, вместо специализированного агрегирующего ответвителя трафика;

− зеркалирующий порт межсетевого экрана.

2.2.10 Сетевой датчик в режиме IPS устанавливается «в разрыв» между сегментом потенциальных нарушителей и защищаемым сегментом.

2.2.11 Для корректного анализа трафика сетевым датчиком, необходимо убедиться, что суммарный пиковый объем трафика, передаваемого через контролируемый сегмент за единицу времени, не превышает пропускной способности сетевого порта, к которому подключен сетевой датчик. В противном случае часть подлежащих анализу данных может быть потеряна.

2.2.12 Если планируется использовать сетевой датчик в режиме IDS и в АИС есть межсетевой экран, то необходимо определить в какой именно точке будет сниматься трафик для анализа (рисунок 2.2.3):

− до межсетевого экрана (со стороны сегмента потенциальных нарушителей), точка 1 на рисунке 2.2.3;

− после межсетевого экрана (со стороны защищаемого сегмента), точка 2 на рисунке 2.2.3;

− в обоих точках одновременно, точка 1 и точка 2 на рисунке 2.2.3.

В случае, если сетевой датчик устанавливается для защиты конкретных информационных ресурсов (уязвимости в которых могут быть отслежены с помощью сетевого датчика и у сетевого датчика есть в наличии соответствующие сигнатуры), находящихся в защищаемой сети и опубликованных для доступа из сети Internet, то месторасположение сетевого датчика не имеет значение.

Однако, следует отметить, что:

− установка датчика до межсетевого экрана (со стороны сегмента потенциальных нарушителей) позволит отследить попытки компьютерных атак на защищаемую сеть, «отбиваемые» межсетевым экраном, что позволяет оценить качество проведенных работ по защите сети, выявить необходимость проведения дополнительных работ;

– установка датчика после межсетевого экрана (со стороны защищаемого сегмента) позволяет оценить работоспособность самого межсетевого экрана, корректность настройки правил на нем, выявить проблемы, находящиеся в самой защищаемой сети (например, если какой-то пользователь подцепил «вирус», который отсылает по электронной почте спам-сообщения).

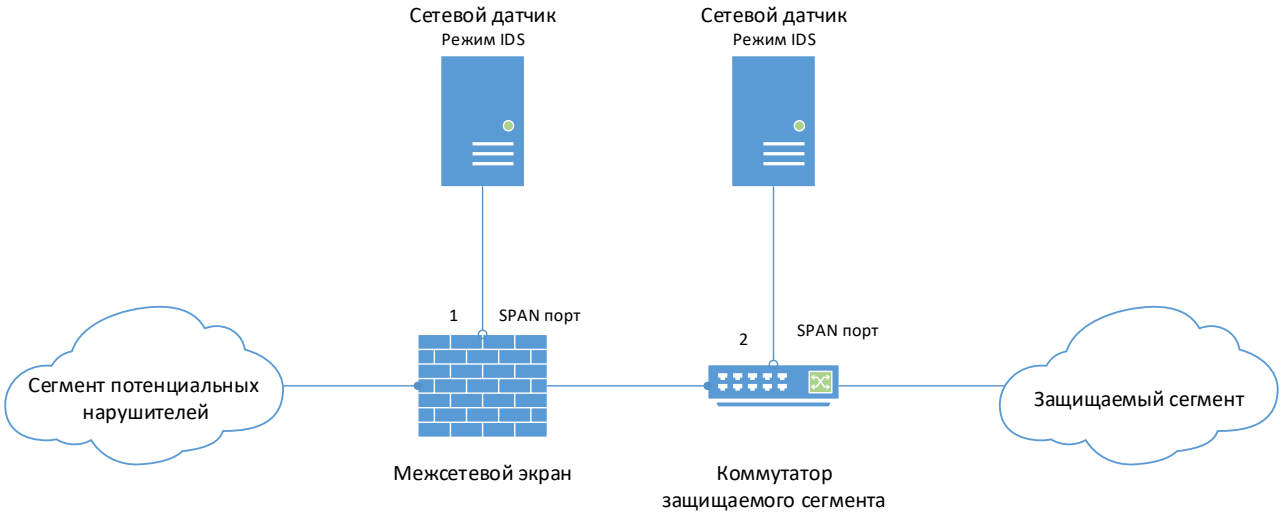

Рисунок 2.2.3 – Схема включения сетевого датчика в режиме IDS при наличии межсетевого экрана

2.2.13 В случае, когда сетевой датчик в режиме IDS планируется устанавливать в АИС, в которой кроме основного имеется резервный коммутатор (например, основной и резервный коммутатор уровня ядра в режиме Active/Passive), основной и резервный криптомаршрутизатор, то в этом случае рекомендуется резервировать сами сетевые датчики: один сетевой датчик (основной) подключается к основному коммутатору, второй (резервный) – к резервному.

2.3 О режимах работы сетевого датчика IDS (Half Duplex, Full Duplex)

2.3.1 Устройство, зеркалирующее трафик для сетевого датчика может работать в следующих режимах:

1) Трафик контролируемого канала связи может копироваться в один зеркалирующий порт. В этом случае этот зеркалирующий порт подключается к сетевому одному интерфейсу сер вера сетевого датчика (далее такой ражим работы сетевого датчика будет именоваться «Half Duplex»).

2) Входящий трафик (rx) контролируемого канала связи копируется в один зеркалирующий порт, а исходящий (tx) в – другой. В этом случае сервер с сетевым датчиком должен иметь два сетевых интерфейса для приема трафика, в которые подключаются зеркалирующие порты.

Указанный режим работы сетевого датчика, далее называемый как Full Duplex, рационально использовать при контроле канала связи с пропускной способностью 1 Гбит/с с помощью двух зеркалирующих сетевых интерфейсов со скоростью 1 Гбит/с.

2.3.2 Как известно, суммарная скорость обмена информацией по каналу связи Gigabit Ethernet со скоростью 1 Гбит/с, работающем в режиме Full Duplex, может быть близка к 2 Гбит/с: 1 Гбит/с – передача и 1 Гбит/с – приём. Для полного съема сетевого трафика с такого канала необходимо использовать:

– 2 зеркалирующих сетевых интерфейса 1 Гбит/с (первый зеркалирует принимаемую информацию, второй – передаваемую) – рисунок 2.3.1 «А)»»;

– 1 зеркалирующий сетевой интерфейс 10 Гбит/с – рисунок 2.3.1 «Б)».

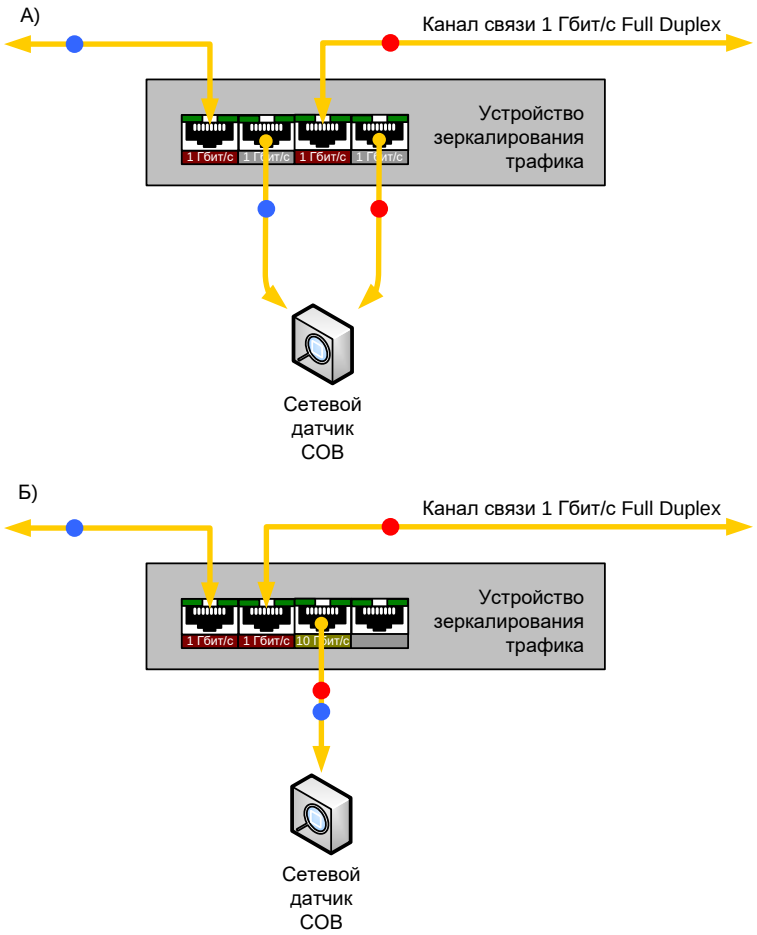

Рисунок 2.3.1 – Обеспечение съёма сетевого трафика в режиме Full Duplex:

А) при использовании двух сетевых портов

Б) при использовании сетевого порта большей производительности.

2.3.3 Использовать зеркалирующий порт с меньшей пропускной способностью можно, если прогнозируемый объем трафика не превысит пропускную способность зеркалирующего пор-

та коммутатора, но при этом следует учитывать, что в случае всплесков сетевой активности часть трафика все-таки не будет попадать на сетевой датчик для анализа.

2.3.4 Поддержка режиме Full Duplex присутствует в сетевом датчике версии 0.2.

2.3.5 Зеркалирование трафика в два сетевых интерфейса с разделением по направлению («на прием» и «на передачу») доступно во многих моделях управляемых коммутаторов (Cisco начиная с модели 3560), а также в специализированных ответвителях трафика (Tap).

2.4 О режимах работы сетевого датчика IPS (af_packet, dpdk)

2.4.1 Сетевой датчик в режиме IPS работает в следующих режимах:

- af_packet, когда интерфейсы настраиваются как обычный сетевой мост;
- dpdk, когда интерфейсы настраиваются с использованием библиотек dpdk, что повышает производительность сетевого датчика при анализе проходящего трафика.

2.4.2 При внедрении сетевого датчика в ваше АИС стоит учитывать, что режим dpdk имеет ряд ограничений в эксплуатации и не подойдет всем системам:

- не все сетевые карты поддерживают режим dpdk. Со списком сетевых карт, поддерживающих dpdk можно ознакомиться на сайте http://dpdk.org/doc/nics;
- режим dpdk поддерживается не всеми виртуальными средами.

3 ВЫЗОВ И ЗАГРУЗКА

3.1 Для обеспечения корректного функционирования системы в первую очередь требуется доступность сервера с базой данных (СУБД). После загрузки сервера с базой данных становится возможной корректная работа Форпост Сервера. Далее к Форпост Серверу подключаются агенты, к которым подключены модули (сетевые датчики, модули контроля целостности, модули управления сетевым оборудованием, хостовые датчики, и к нему же возможно подключение Форпост Клиента администратора системы.

3.2 Порядок запуска компонентов системы не имеет значения: в случае, если какой-либо компонент системы, необходимый для работы выбранного компонента не доступен, выбранный компонент в цикле ожидает появление доступности необходимого компонента.

3.3 При правильном старте базовых компонентов системы Форпост Клиент должен подключаться к Форпост Серверу, предварительно проведя аутентификацию пользователя.

3.4 ПО системы реализовано как набор исполняемых файлов и библиотек (таблицы 3.1 и 3.2 соответственно).

3.5 Все компоненты системы используют динамическое выделение памяти, производя ее выделение по необходимости и освобождая при окончании работы.

3.6 Программы, реализованные в виде сервисов (Форпост Агент, Форпост Сервер, модули) запускаются с помощью Service Control Manager (SCM), входящего в состав общесистемного программного обеспечения.

3.7 Форпост Клиент запускается пользователем.

Таблица 3.1 – Исполняемые файлы

Имя файла	Описание
forpostagentd	Исполняемый файл Форпост Агента
forpostclient	Исполняемый файл Форпост Клиента
hostsensord	Исполняемый файл Хостового дотчика
dataintegritysensord	Исполняемый файл Датчика контроля целостности
NetworkSensor	Исполняемый файл Сетевого датчика
ScriptGen	Исполняемый файл генератора динамических скриптов БД
forpostserverd	Исполняемый файл Форпост Сервера
forpostfcmd	Исполняемый файл Модуля управления сетевым оборудованием

Таблица 3.2 – Файлы библиотек

libapr-1.so	Библиотека APR
libaprutil-1.so	Утилиты библиотеки APR
libapriconv-1.so	Компонент iconv библиотеки APR
liblog4cxx.so	Библиотека log4cxx (для логирования)
libiconv.so	Библиотека libiconv
libcharset.so	Библиотека компилятора libarset
libQtCore.so	Ядро библиотеки Qt
libQtNetwork.so	Компонент библиотеки Qt для реализации сетевых функций
libQtGui.so	Компонент библиотеки Qt для отображения графических элементов
libQtXml.so	Компонент библиотеки Qt для работы с XML
libQtSvg.so	Компонент библиотеки Qt для работы с SVG
libQtWebKit.so	Компонент библиотеки Qt для предоставления динамического web-контента
libQtXmlPatterns.so	Компонент библиотеки с Qt, обеспечивающий корректную работу с XPath, XQuery, XSLT и XML-схемами
libqwt.so	Библиотека QWT
libqwtmathml.so	Компонент библиотеки QWT – текстовый движок для рендеринга MathML
libgvc.so	Контекстная библиотека GraphViz
libcdt.so	Библиотека контейнеров типов данных GraphViz
libcgraph.so	Библиотека, работающая с хранением, обработкой и чтением/записью графов GraphViz
libxdot.so	Библиотека, предназначенная для отображения ориентированных графов в GraphViz
libpathplan.so	Библиотека, определяющая наикратчайшие пути в многоугольниках, используется GraphViz
libxml2.so	Библиотека libxml2
libboost_serialization-mt.so	Компонент для сериализации библиотеки Boost
libboost_wserialization-mt.so	Расширенный компонент для сериализации библиотеки Boost
libboost_system-mt.so	Компонент для работы приложений с ошибками системы библиотеки Boost
libboost_program_options-mt.so	Компонент для настройки приложений библиотеки Boost

libboost_thread-mt.so	Компонент для управления многопоточностью библиотеки Boost
libboost_chrono-mt.so	Компонент для работы с системным временем библиотеки Boost
libboost_filesystem-mt.so	Компонент для работы с файловой системой библиотеки Boost
libboost_regex-mt.so	Компонент для с регулярными выражениями библиотеки Boost
libboost_date_time-mt.so	Компонент для управления временем и датой библиотеки Boost
libboost_locale-mt.so	Компонент для локализации приложений библиотеки Boost
libboost_signals-mt.so	Компонент для управления сигналами библиотеки Boost
libomniORB4.so	Библиотека omniORB
libomnithread.so	Библиотека omnithread
libomnisslTP4.so	Компонент omniORB для поддержки SSL
libomniDynamic4.so	Компонент omniORB
libInstallHelperLibrary.so	Вспомогательная библиотека для установки
libnghttp2.so	Библиотека nghttp2
libluajit-5.1.so	Библиотека luajit
libdnet.1	Библиотека libnet
libsfbpf.so	Библиотека DAQ (компонент, реализующий BPF)
libpcap.so	Библиотека PCAP
libPocoFoundation.so	Библиотека Poco
libPocoUtil.so	Утилиты библиотеки Poco
libPocoJSON.so	Компонент библиотеки Poco для поддержки формата JSON
libPocoXML.so	Компонент библиотеки Poco для поддержки формата XML
libPocoNet.so	Компонент библиотеки Poco для для работы с сетями
libPocoNetSSL.so	Компонент библиотеки Poco для поддержки SSL
libPocoCrypto.so	Компонент библиотеки Poco для поддержки криптографии
libTelnetClient.so	Telnet-клиент
libTelnetClientSSPT2.so	Telnet-клиент SSPT2
libUDPClient.so	UDP-клиент
libSnmpServer.so	SNMP-сервер

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Входные данные

4.1.1 Для всех без исключения компонентов системы Форпост одним из пунктов требуемых входных данных является конфигурационный файл forpost.xml, в котором содержатся необходимые для функционирования системы настройки.

4.1.2 Входными данными для компонента **«Форпост Сервер»** являются сообщения модулей и датчиков, переданные через агенты, конфигурационный файл Форпост Сервера, передаваемые из Форпост Клиента хранимые процедуры.

4.1.3 Для компонента «**Форпост Клиент**» являются данные о записях в журналах. Также в Форпост Клиент передаются данные о пользователях, данные о ролях, данные о зонах, данные о событиях, данные об отчетах.

4.1.4 Для компонента «**Форпост Агент**» входными данными являются сообщения модулей и датчиков, которые поступают через Pipe.

4.1.5 Для компонента «**Датчик контроля целостности**» входными данными является подписанный файл списка контролируемых файлов, сертификат ЦС, последний базовый список отзыва, выписанный для данного хоста сертификат.

4.1.6 Для компонента «**Сетевой датчик**» входными данными является трафик, снимаемый с зеркалирующего порта коммутатора (межсетевого экрана, специализированного ответвителя трафика (TAP) и др).

4.1.7 Для компонента «**Форпост Экспорт**» входными данными являются записи из бузы данных, предназначенные для отправки в SIEM.

4.1.8 В процессе работы компонента **«Хостовой датчик»** в системе собирается следующая информация:

- Текущий активный пользователь в ОС, без истории;
- Информация об ОС, версия, память, процессор;
- Информация о жестких дисках (в том числе внешних);
- События счетчиков (логи);
- События системы: установка/удаление любых пакетов.

4.1.9 Данные в компонент **«Модуль управления сетевым оборудованием»** могут поступать либо по протоколу SNMP, либо по протоколу SYSLOG (в этом случае для отправки используется UDP).

При получении сообщения SYSLOG производится попытка разбора сообщения по следующему шаблону:

```
------------------------------------------------------------
% [символы] :
тип сообщения
>
порядковый номер месяца (считая январь 0)
день месяца
число лет начиная с 1900
число часов (от 0 до 23)
число минут (от 0 до 59)
число секунд (от 0 до 59)
тело сообщения
------------------------------------------------------------
```

Тело сообщения заносится в журнал сообщений сетевого оборудования. Если не удается разобрать сообщение, то оно целиком заносится в журнал сообщений сетевого оборудования.

Оборудования Cisco может отправлять по протоколу SNMP сообщения, которые обычно отправляются по протоколу SYSLOG. В этом случае сначала к сообщению применяется процедура разбора для сообщений SNMP, после чего применяется процедура разбора для сообщений SYSLOG.

Входными данными является набор управляющих и информационных символов для управления VT220 терминалом, которым и является терминал управления сетевым оборудованием в консоли администратора.

Модуль управления сетевым оборудованием поддерживает выполнение команд блокировки и разблокировки для сетевого оборудования.

4.2 Выходные данные

4.2.1 Для компонента «**Форпост Сервер**» выходными данными являются результаты хранимых процедур, принимаемых от компонента «Форпост Клиент» и прочих компонентов и выполняемых в базе данных.

4.2.2 Для компонента «**Форпост Клиент**» выходными данными является отображаемая в журналах и графиках информация, настройки системы.

4.2.3 Для компонента «**Форпост Агент**» выходными данными являются сообщения модулей, которые поступают в БД, а также сообщения о статусе подключенных к Форпост Агенту компонентов.

4.2.4 Для компонента «**Датчик контроля целостности**» выходными данными является информация, передаваемая датчиком в базу данных о состоянии целостности контролируемых файлов, а также сообщения об успешном или неуспешном обновлении списка контролируемых файлов.

4.2.5 Для компонента «**Сетевой датчик**» выходными данными является информация, передаваемая датчиком в базу данных о сетевой активности, зафиксированной данным датчиком в зависимости от его настроек.

4.2.6 Для компонента «**Форпост Экспорт**» выходными данными являются UDP-сообщения, содержащие записи из БД.

4.2.7 Для компонента «**Хостовой датчик**» выходными данными является информация, передаваемая датчиком в базу данных о состоянии контролируемого компьютера.

4.2.8 Компонент «**Модуль управления сетевым оборудованием**» пересылает сетевому оборудованию простейшие символы, генерируемые в результате нажатия клавиш в терминале управления, или целые строчки, полученные из буфера обмена. Также пересылаются команды блокировки и разблокировки для сетевого оборудования. Формат команд блокировки/разблокировки определяется видом сетевого оборудования, и считывается из xml файла, указанного в конфигурационном файле (параметр TelnetClient.TemplateFileNameFull). Вся информация для сетевого оборудования пересылается по протоколам telnet или RS-232.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий номер сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					