АО «РНТ»

Утвержден
РМАГ.00026-24 31 01-ЛУ

СИСТЕМА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК «ФОРПОСТ»

Версия 2.0.1

Описание применения

РМАГ.00026-24 31 01

Листов 32

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2016

АННОТАЦИЯ

Настоящий документ содержит описание применения системы обнаружения компьютерных атак «Форпост» версии 2.0 (2.0.1). В документе описываются назначение и функциональность продукта, его характеристики, системные требования, особенности применения. Так же приведены описание логической структуры, требования к окружению, в котором должна функционировать СОА, типовая схема включения СОА в типовую автоматизированную информационную систему; описана методика проектирования аппаратного обеспечения для работы СОА, приведены условия применения сетевого датчика СОА для достижения максимальной производительности.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и функциональность продукта

1.1.1 Система обнаружения компьютерных атак (СОА) «Форпост», предназначена для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему (АИС), которые могут быть классифицированы как компьютерные атаки.

1.1.2 СОА «Форпост» обеспечивает:

− обнаружение компьютерных атак, направленных на сервера телематических служб (WEB, FTP, электронная почта, СУБД и пр.) и рабочие станции, размещенные в контролируемых сегментах АИС;

− предотвращение развития сетевых компьютерных атак путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору), по протоколам RS-232, telnet, соответствующей последовательности команд на основе шаблонов;

− оповещение администратора безопасности об обнаруженных атаках 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 так же, за счет этого механизма, возможность отслеживания действий нарушителей по отношению к контролируемым ресурсам в скомпрометированной системе;

− оповещение администратора безопасности о новых сообщениях системных журналов на машинах защищаемой АИС путем вывода соответствующего сообщения на консоль администратора СОА, записи сообщения в специальный журнал, путем отправки сообщений по электронной почте;

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

− удаленное управление сетевым оборудованием по защищенному с использованием отечественных средств криптографической защиты информации (СКЗИ) каналу;

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

− генерацию отчетов на основе содержимого журналов СОА.

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

1.2 Характеристики продукта

1.2.1 В основу функционирования сетевого датчика СОА «Форпост» положен сигнатурный метод выявления атак. Он обеспечивает обнаружение атак на основе специальных шаблонов (сигнатур), каждый из которых соответствует конкретной атаке. При получении исходных данных о сетевом трафике информационной системы, СОА «Форпост» производит их анализ на соответствие указанным шаблонам атак, имеющихся в базе данных.

В случае обнаружения сигнатуры в исходных данных, система регистрирует факт обнаружения атаки, оповещает администратора безопасности о данном событии и предоставляет возможность администратору произвести блокирование источника атаки с помощью соответствующего коммуникационного оборудования.

За счет использования датчиков контроля целостности СОА позволяет отслеживать действия нарушителя по отношению к контролируемым ресурсам в скомпрометированной системе.

Дополнительно поддерживается получение данных о функционировании отдельных объектов контролируемой АИС по протоколам syslog и SNMP.

1.2.2 СОА «Форпост» реализует следующие методы реагирования на факт выявления компьютерной атаки:

- идентификация компьютерной атаки с использованием описаний уязвимостей, на которые они направлены, или описаний реализаций компьютерных атак;
- оповещение администратора безопасности об обнаруженных атаках путем вывода соответствующего сообщения на консоль администратора СОА, отправки сообщений по электронной почте;
- регистрация атаки в журнале модулей-датчиков СОА;
- блокировка источника угрозы информационной безопасности путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору), по протоколам RS-232, telnet, последовательности команд на основе шаблонов.

Управление сетевым оборудованием производится компонентом СОА через локальный интерфейс RS-232 или через выделенный сетевой интерфейс с использованием протокола telnet. Связь между удаленной консолью администратора и компонентом СОА, выполняющим управление сетевым оборудованием осуществляется по защищенному с использованием отечественных СКЗИ каналу.

1.2.3 СОА «Форпост» обеспечивает возможность выборочного контроля ресурсов защищаемой АИС, контроль целостности собственных ресурсов (исполняемых и конфигурационных файлов, веток реестра) СОА и ресурсов защищаемой АИС. Также СОА «Форпост» позволяет получать новые сообщения системных журналов контролируемой АИС.

1.2.4 СОА «Форпост» имеет консоль администратора, которая реализует механизм удаленного управления данным средством. Дополнительно система имеет механизм локального управления, позволяющий: производить настройку своих компонентов, их запуск, остановку и перезапуск; формировать, редактировать и подписывать электронной цифровой подписью администратора СОА список контролируемых на целостность ресурсов.

1.2.5 С целью маскирования СОА «Форпост» в составе контролируемой АИС предполагается выделение СОА в отдельный сегмент, если на защищаемых объектах не установлены датчики контроля целостности, или отделение компонентов СОА от возможных нарушителей с помощью межсетевых экранов, исключая точки съема информации сетевыми датчиками.

В качестве дополнительной меры по затруднению демаскирования компонентов СОА предусмотрена возможность наложения ограничений на сетевые адреса, между которыми осуществляется взаимодействие компонентов.

1.2.6 СОА «Форпост» реализует следующие механизмы собственной защиты:

− обеспечивается идентификацию и аутентификацию администратора СОА при запуске консоли администратора по имени пользователя и паролю; ведется контроль длины создаваемых паролей (не менее 6 символов) и состав паролей (буквенно-цифровые);

− в процессе работы осуществляется контроль целостности компонентов и конфигураций СОА;

− СОА имеет функцию сигнализации администратору СОА о неверных попытках аутентификации при доступе к консоли администратора, в частности, сигнализации о трех подряд неверных попытках аутентификации путем записи соответствующего события в системный журнал и отсылки сообщения электронной почты;

− управляющая информация, служебная информация компонентов и данные о выявленных компьютерных атаках могут передаваться между компонентами в зашифрованном виде с использованием СКЗИ КриптоПро 3.6 или СКЗИ КриптоПро 3.6.1 (КриптоПро 3.6 R4) по протоколу TLS;

− предусмотрена возможность наложения ограничений на адреса, с которых осуществляется удаленное администрирование СОА.

1.2.7 СОА «Форпост» имеет автоматизированный механизм обновления базы решающих правил, позволяющий загружать сигнатуры компьютерных атак на датчики, с использованием консоли администратора.

Дополнительно имеются штатные средства задания новых сигнатур компьютерных атак с использованием языка описания сигнатур.

1.2.8 СОА «Форпост» регистрирует в своих журналах:

- сведения о выявленных компьютерных атаках и случаях нарушения целостности контролируемых ресурсов;
- сведения о сообщениях системных журналов с машин контролируемых ресурсов.
- служебную информацию, формируемую компонентами СОА, такую как подключение или отключение компонентов СОА, вход и выход администратора СОА в консоль администратора, информацию о блокировке или разблокировке источника атаки и пр.
- сообщения от сетевого оборудования, поступающие по протоколам SNMP и syslog.

СОА «Форпост» имеет функцию периодического создания резервных копий базы данных СОА в отдельный файл с последующим выводом соответствующего сообщения на консоль администратора СОА.

1.2.9 Дополнительные характеристики СОА «Форпост»:

- имеет механизм фильтрации событий, отображаемых в журналах СОА;
- обладает интуитивно-понятным русскоязычным графическим интерфейсом администрирования;
- работает под управлением операционных систем семейства Windows;
- обеспечивает анализ стека протоколов TCP/IP, начиная с канального уровня;
- реализует поддержку MPLS, VLAN;
- поддерживает интеграцию с внешними системами (например, с различными системами корреляции: Cisco Mars, ArcSight и др.) путем отсылки сообщений о компьютерных атаках из журнала СОА по протоколу syslog;
- имеет возможность генерации табличных и текстовых отчетов на основе содержимого журналов СОА;
- имеет распределенную модульную архитектуру, обеспечивающую масштабируемость системы, позволяющую адаптироваться под требования конкретной АИС по производительности и отказоустойчивости;
- существует возможность резервирования ключевых компонентов.

1.3 Системные требования

1.3.1 СОА «Форпост» предъявляет следующие минимальные системные требования:

- операционная система Windows Server 2003/2008/2012/XP/7/8;

Примечания

1 Для информационного фонда, координационного центра и сетевого датчика необходимо использовать серверные редакции ОС Windows. Использование клиентских редакций ОС Windows для указанных компонентов, как правило, приводит к снижению их производительности и допускается только при соблюдении лицензионных ограничений указанных ОС.

2 Для корректной работы компонента «Консоль администратора» (файл ConsoleAdmin.exe) и оснастки настройки СОА «Форпост», расположенной в области уведомлений (системном трее) (файл TrayController.exe), требуются права администратора. Если прав текущего пользователя не хватает для работы указанных компонентов – автоматически будет появляться окно ввода пароля администратора. Так же можно отключить в ОС Windows контроль учётных записей пользователей (англ. User Account Control, UAC). Для этого необходимо в панели управления выбрать пункт «Изменение параметров контроля учетных записей». Переместить ползунок, расположенный в левой части появившегося окна, в самое нижнее положение («Никогда не уведомлять»), нажать кнопку «ОК» и перезагрузить компьютер.

Требования к аппаратному обеспечению:

- процессор с частотой не менее 1,6 ГГц;
- оперативной памяти не менее 2 ГБ;
- объем свободного дискового пространства не менее 20 ГБ;
- сетевой интерфейс со скоростью не менее 100 Мбит/с;
- на сервере с сетевым датчиком – дополнительно не менее 1 сетевого интерфейса для захвата трафика со скоростью не менее 100 Мбит/с, предпочтительно, в серверном исполнении.

1.3.2 Поскольку система распределенная, компоненты СОА могут быть установлены как на один сервер, так и распределены на несколько физических серверов.

1.3.3 При повышенных требованиях по производительности рекомендуется:

- на серверах с информационным фондом, координационными центрами, сетевыми датчиками увеличить тактовую частоту процессора и использовать многоядерные, либо многопроцессорные конфигурации; использовать серверные версии операционной системы Windows;
- на серверах с сетевыми датчиками увеличить объем оперативной памяти до 16 ГБ;
- привести объем дискового пространства в соответствие с потребностями информационного фонда по объему единовременно хранимой в системе информации о событиях;
- на серверах с сетевыми датчиками для захвата трафика использовать сетевые интерфейсы со скоростью 1 или 10 Гбит/с в серверном исполнении.

Дополнительные сведения о выборе аппаратной конфигурации для компонентов СОА «Форпост» в зависимости от требований по производительности приведены в п. 2.5 данного документа.

1.4 Особенности применения продукта

1.4.1 СОА «Форпост» имеет следующие особенности применения:

− необходимо своевременно проводить техническое обслуживание системы в соответствии с регламентом, описанном в руководстве администратора, РМАГ.00026-24 90 01;

− уведомление администратора о возникновении ситуации, требующей его внимания, возможно через консоль администратора, всплывающее окно, по электронной почте;

− хранение всей накопленной системой информации о процессах в АИС 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 резервное копирование и удаление несущественной информации (одновременно консоль администратора в журнале модулей-датчиков может выводить на экран не более 100 000 записей);

− размер буфера у агентов, в котором они накапливают информацию, полученную от датчиков и подлежащую отправке в координационный центр, фиксированный и информация в нем обновляется циклически (старые события, подлежащие отправке в координационный центр по достижению максимального размера буфера затираются более новыми), что в случае недостаточной пропускной способности канала связи (или каких-либо других факторов) может приводить к потере части данных;

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

2 ОПИСАНИЕ УСЛОВИЙ ПРИМЕНЕНИЯ

2.1 Описание логической структуры системы

2.1.1 СОА «Форпост» имеет распределенную многомодульную архитектуру (логическая структура СОА «Форпост» представлена на рисунке 2.1). Модули могут быть установлены как на один сервер, так и распределены на несколько в зависимости от требуемых показателей производительности и отказоустойчивости.

2.1.2 Рассмотрим каждый компонент более подробно.

2.1.2.1 **Информационный фонд** представляет собой базу данных, работающую под управлением СУБД MS SQL 2005/2008/2012/2014, специальный компонент «Агент БД», и обеспечивает:

- централизованное хранение событий системы;
- централизованное хранение шаблонов датчиков и базы сигнатур СОА.

Компонент «Агент БД» в связке с **CryptoODBC-драйвером** из состава СОА «Форпост» обеспечивает криптографически защищенный с использованием отечественных СКЗИ информационный обмен между информационным фондом и компонентами СОА, которые к нему подключаются (координационный центр, модуль почтовых уведомлений).

2.1.2.2 **Координационный центр** является связующим звеном между модулями системы: обеспечивает передачу информации между ними, выполняет функции контроля работоспособности компонентов.

2.1.2.3 **Консоль администратора** обеспечивает пользовательский интерфейс и позволяет:

- 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 журнале модулей-датчиков;
- 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.

2.1.2.4 **Модуль интеграции с сетевым оборудованием** состоит из следующих функциональных модулей.

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

2) Модуль приема сообщений от сетевых устройств – 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.

3) Модуль интеграции с внешними системами – предоставляет возможность экспорта сообщений, поступающих в журнал датчиков СОА, в различные внешние системы корреляции и мониторинга (такие как Cisco Mars, ArcSight и др.).

Модуль интеграции с сетевым оборудованием предназначен для:

− установления и поддержания подключения к сетевому оборудованию (межсетевые экраны, коммутаторы, маршрутизаторы) по протоколам RS-232, telnet;

− управления сетевым оборудованием (блокировка источников угроз на основе ранее написанных шаблонов, ручное управление);

− получения системных сообщений от сетевого оборудования (по протоколам SNMP и syslog);

− интеграции с внешними системами (например, с различными системами корреляции: Cisco Mars, ArcSight и др.) путем отсылки сообщений о компьютерных атаках из журнала СОА по протоколу syslog.

2.1.2.5 **Модуль почтовых уведомлений** позволяет автоматически по электронной почте отправлять заранее заданным адресатам информацию об обнаруженных атаках и событиях, происходящих в системе.

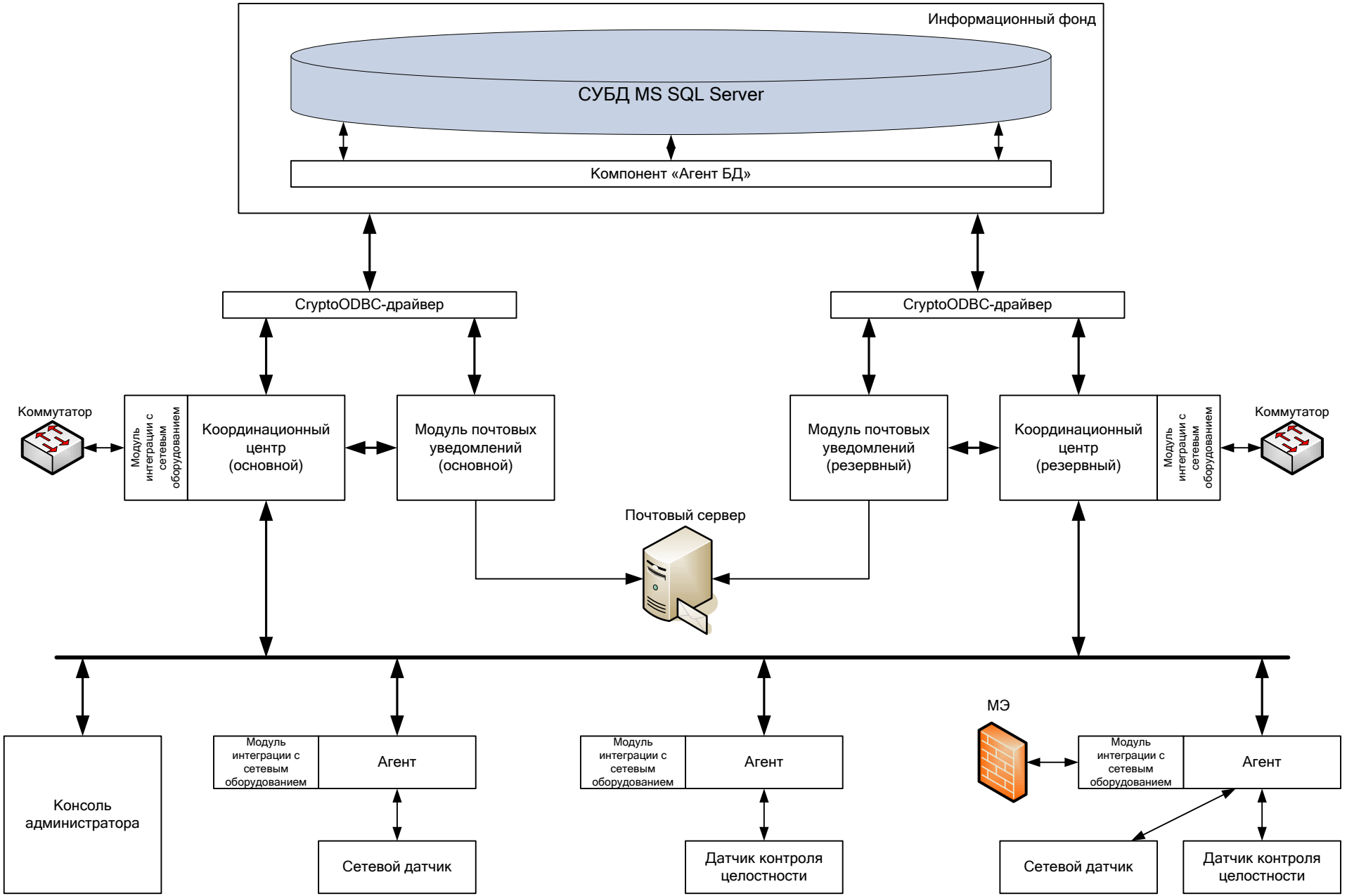

Рисунок 2.1 – Логическая структура СОА «Форпост»

2.1.2.6 **Агент** выполняет функции управления датчиками, а также функции обеспечения передачи информации между датчиками и координационным центром. К одному агенту может быть подключен один датчик контроля целостности и несколько сетевых датчиков.

2.1.2.7 **Сетевой датчик** осуществляет анализ поступающего трафика на наличие в нем компьютерных атак используя сигнатурный метод; подключается к зеркалирующему (SPAN) порту коммутатора, межсетевого экрана, специализированного ответвителя трафика (TAP) и пр.

2.1.2.8 **Датчик контроля целостности** производит контроль целостности собственных ресурсов (исполняемых и конфигурационных файлов, веток реестра) СОА и ресурсов защищаемой АИС. Также датчик контроля целостности отслеживает появление новых сообщений системных журналов.

2.1.2.9 Компоненты Информационный фонд, Координационный центр, Консоль администратора, Модуль интеграции с сетевым оборудованием, Модуль почтовых уведомлений, Агент, Датчик контроля целостности образуют **Центр управления** СОА «Форпост».

2.1.3 Взаимодействие компонентов СОА «Форпост» друг с другом происходит по следующей схеме.

2.1.3.1 Главным связующим звеном между компонентами системы является координационный центр, осуществляющий передачу следующей информации между информационным фондом и остальными компонентами:

− данные о зафиксированных событиях (включая результаты работы) и состоянии компонентов;

− шаблоны датчиков и база сигнатур СОА.

Существует возможность резервирования координационного центра (и модуля почтовых уведомлений, который ставится на один сервер с ним).

2.1.3.2 По умолчанию предполагается, что связь координационных центров с СУБД информационного фонда будет осуществляться с использованием ODBC-драйвера из состава СОА «Форпост» (CryptoODBC-драйвер).

ODBC-драйвер из комплекта поставки операционной системы или СУБД подключается непосредственно к СУБД. ODBC-драйвер из состава СОА «Форпост» (CryptoODBC-драйвер) подключается к СУБД через компонент «Агент БД». Компонент «Агент БД» подключается к СУБД через ODBC-драйвер из комплекта поставки операционной системы или СУБД.

Использование ODBC-драйвера из состава СОА «Форпост» вместо драйвера из комплекта поставки операционной системы или СУБД является обязательным, если предполагается шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов.

Допускается использование ODBC-драйвера из комплекта поставки операционной системы или СУБД в случае, если информационный фонд и координационный центр предполагается устанавливать на одном сервере, а так же в случае, если шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов не требуется.

2.1.3.3 Управление датчиками СОА и передача информации между датчиками и координационными центрами осуществляется агентами. Агенты устанавливаются на каждый сетевой узел, на котором установлены любые датчики СОА «Форпост» (сетевой датчик, датчик контроля целостности).

2.1.3.4 Для обеспечения контроля целостности компонентов СОА «Форпост», датчик контроля целостности устанавливается на каждый сетевой узел, на котором установлены компоненты СОА «Форпост». Дополнительно датчик контроля целостности устанавливается на узлы защищаемой АИС с целью контроля целостности ресурсов защищаемой АИС, возможности отслеживание действий нарушителей по отношению к контролируемым ресурсам в скомпрометированной системе а также для отслеживания появления новых сообщений системных журналов.

2.1.3.5 Входными данными сетевого датчика является трафик, снимаемый с зеркалирующего порта коммутатора (межсетевого экрана, специализированного ответвителя трафика (TAP) и др.)

2.1.3.6 Консоль администратора подключается непосредственно к координационному центру, от которого она получает данные о состоянии компонентов и результаты их работы. С консоли администратора может производиться удаленная установка, удаление, конфигурирование компонентов СОА, управление ими.

2.1.3.7 Модуль почтовых уведомлений служит для автоматической отправки отчетов по электронной почте и должен подключаться к внешнему почтовому серверу.

Данный модуль получает данные непосредственно из информационного фонда, но рассылает только ту информацию, которая была передана от датчиков тем координационным центром, за который установлен данный модуль почтовых уведомлений. Подобный алгоритм работы позволяет исключить дублирование информации, передаваемой по электронной почте от нескольких модулей почтовых уведомлений, установленных на различных координационных центрах.

2.1.3.8 Функциональность модуля интеграции с сетевым оборудованием интегрирована в агент и координационный центр. Таким образом, существует возможность управлять сетевым оборудованием, подключенным локально к узлам, на которые установлены указанные выше модули СОА.

2.2 Требования к окружению

2.2.1 Для работы информационного фонда СОА «Форпост» на серверах, предназначенных для его установки, должна быть развернута система управления базами данных (СУБД) MS SQL 2005/2008/2012/2014.

2.2.2 Для использования в подсистеме собственной безопасности СОА «Форпост» отечественных криптоалгоритмов, на все узлы, на которые установлены компоненты СОА, требуется установка внешнего крипропровайдера. В настоящее время поддерживается работа со средством криптографической защиты информации (СКЗИ) КриптоПро CSP 3.6 и КриптоПро CSP 3.6.1.

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

2.3 Типовая схема включения СОА в автоматизированную информационную систему

2.3.1 Типовая схема включения СОА «Форпост» в автоматизированную информационную систему представлена на рисунке 2.2.

2.3.2 Предполагается, что защищаемая сеть имеет несколько сегментов, разделенных межсетевыми экранами и подключение во внешнюю сеть. Узлы, на которые устанавливаются компоненты СОА «Форпост» (за исключением датчиков контроля целостности) выделяются в отдельный сегмент. Таким образом, в типовой сети имеется три сегмента:

- сегмент серверов;
- сегмент пользователей;
- сегмент СОА «Форпост».

2.3.3 На сервера и АРМ пользователей защищаемой сети устанавливается датчик контроля целостности СОА «Форпост». Также датчик контроля целостности устанавливается на все узлы, на которых установлены компоненты СОА «Форпост».

2.3.4 В сегменте СОА «Форпост» устанавливаются: информационный фонд, координационные центры (основной и резервный) совместно с модулями почтовых уведомлений (основной и резервный), сетевые датчики. В этом же сегменте должна быть установлена консоль администратора. Данные компоненты могут быть установлены как на один сервер, так и распределены на несколько физических серверов.

2.3.5 Функциональность модуля интеграции с сетевым оборудованием интегрирована в компоненты агент и координационный центр, поэтому управление сетевым оборудованием (модуль управления сетевым оборудованием) возможно с любого узла, на котором установлены ком-

поненты агент и координационный центр. На рисунке 2.2 предполагается, что управление ведется с узлов, на которые установлен сетевой датчик (агент обязательно устанавливается перед установкой сетевого датчика).

Сбор информации от сетевого оборудования по протоколам SNMP и syslog (модулем приема сообщений от сетевых устройств), взаимодействие с внешними системами по протоколу syslog (модулем интеграции с внешними системами) может вестись с любого узла, на котором установлены компоненты агент и координационный центр (при установке на межсетевом экране соответствующих разрешающих правил).

Необходимо учитывать, что при настройке модуля интеграции с внешними системами на агенте, по протоколу syslog на внешний syslog-сервер передаются только те сообщения, которые генерируются датчиками, расположенными на данном агенте. Аналогичная ситуация происходит при настройке модуля интеграции с внешними системами на координационном центре: на внешний syslog-сервер передаются только те сообщения, которые пересылались через данный координационный центр. Эту особенность необходимо учитывать при реализации схемы резервирования координационного центра.

2.3.6 Координационный центр устанавливается совместно с модулем почтовых уведомлений. Подключение модуля почтовых уведомлений к информационному фонду происходит напрямую минуя координационный центр. Однако каждый модуль почтовых уведомлений отсылает по электронной почте события только того КЦ, на котором он установлен. Это позволяет избавиться от дублирования сообщений от основного и резервного модуля почтовых уведомлений.

Предполагается, что почтовые уведомления будут отсылаться на почтовый сервер, расположенный в сегменте серверов (при установке на межсетевом экране соответствующих разрешающих правил).

2.3.7 В качестве точки включения в АИС для сетевого датчика могут выступать:

− зеркалирующий порт коммутатора (SPAN-порт) (точки 1 и 2 на рисунке 2.2); коммутатор при этом настраивается таким образом, чтобы пакеты, поступающие на его порты, копировались в зеркалирующий порт;

− контролирующий порт (Monitor port) специализированного агрегирующего ответвителя трафика (Aggregator Tap) (точка 3 на рисунке 2.2), который устанавливается «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика СОА;

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

− зеркалирующий порт межсетевого экрана.

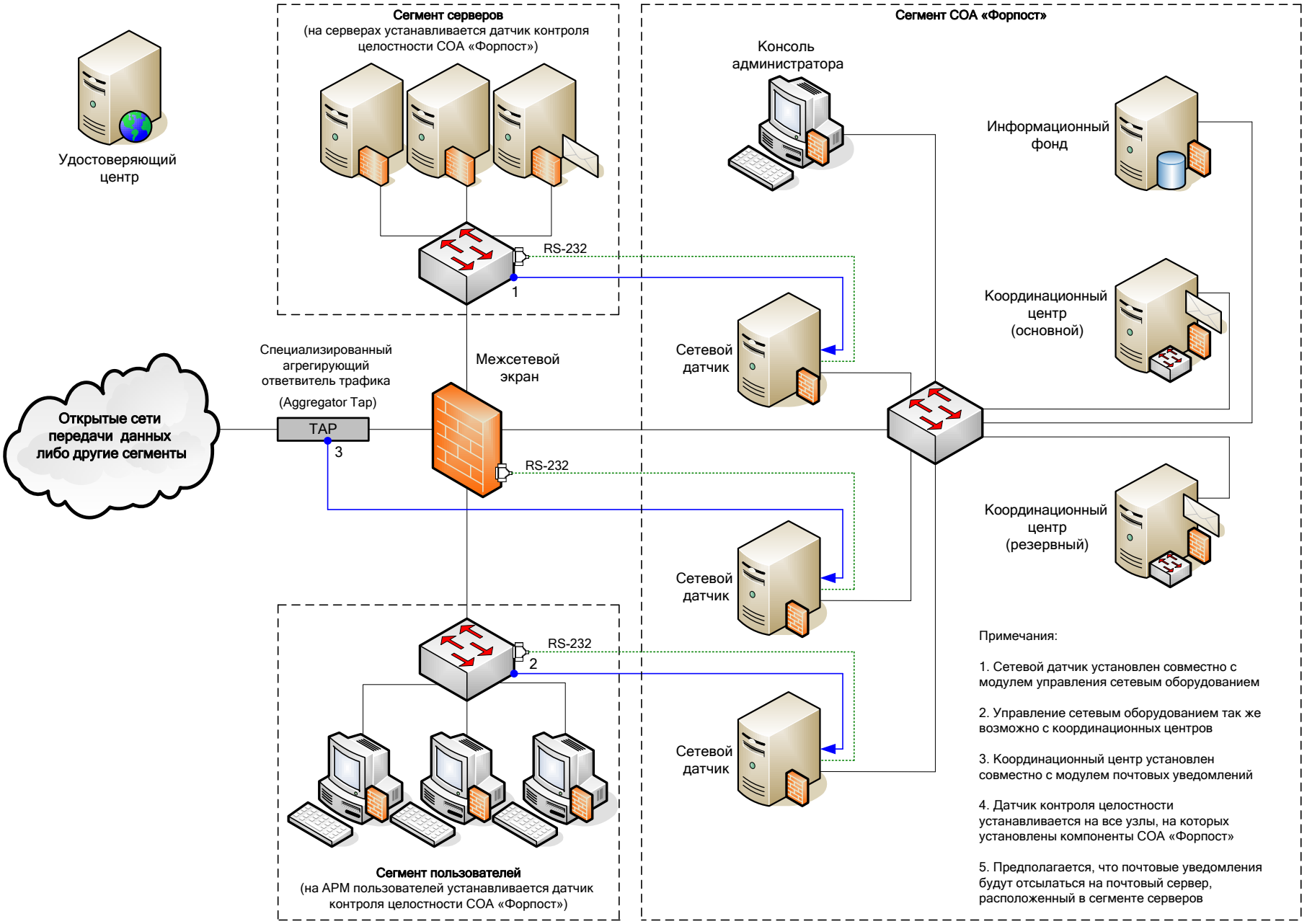

Рисунок 2.2 – Типовая схема включения СОА «Форпост» в автоматизированную информационную систему

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.

2.3.8 Для определения точки включения сетевых датчиков в защищаемую сеть необходимо провести анализ информационных потоков. Проведем такой анализ на примере корпоративной сети, построенной на основе трехуровневой модели (рисунок 2.3). В составе такой сети есть ядро (магистральный уровень), уровень распределения и уровень доступа. В реальной сети, в зависимости от ее размеров и принятых проектных решений, некоторые уровни могут отсутствовать, однако инфорамционные потоки остаются теми же самыми.

2.3.9 В корпоративной сети можно выделить следующие информационные потоки (на рисунке 2.3 отмечены цифрами):

1) Информационный поток между серверами и локальными пользователями (поток № 1).

2) Информационный поток между удаленными пользователями и корпоративной сетью (делится на два подпотока: между удаленными пользователями и серверами; между удаленными пользователями и локальными пользователями) (поток № 2).

3) Информационный поток между корпоративной сетью и, ресурсами и пользователями, находящимися в открытых сетях передачи данных, таких как сеть Internet (делится на два подпотока: между пользователями (как локальными, так и удаленными) и сетью Internet; между серверами и сетью Internet) (поток № 3).

4) Информационный поток между локальными пользователями (поток № 4).

5) Информационный поток между серверами (поток № 5).

2.3.10 Нарушитель, который может повлиять на конфиденциальность, целостность и доступность информации (и информационных ресурсов), обрабатываемой в корпоративной сети может находиться:

- среди локальных пользователей;
- среди удаленных пользователей;
- в открытых сетях передачи данных, таких как сеть Internet.

2.3.11 Следует отметить, что даже если пользователи корпоративной сети не являются нарушителями, они могут нецеленаправленно совершать действия, которые могут повлиять на безопасность корпоративной сети (например – вставить в компьютер носитель USB-Flash, содержащий вирусы).

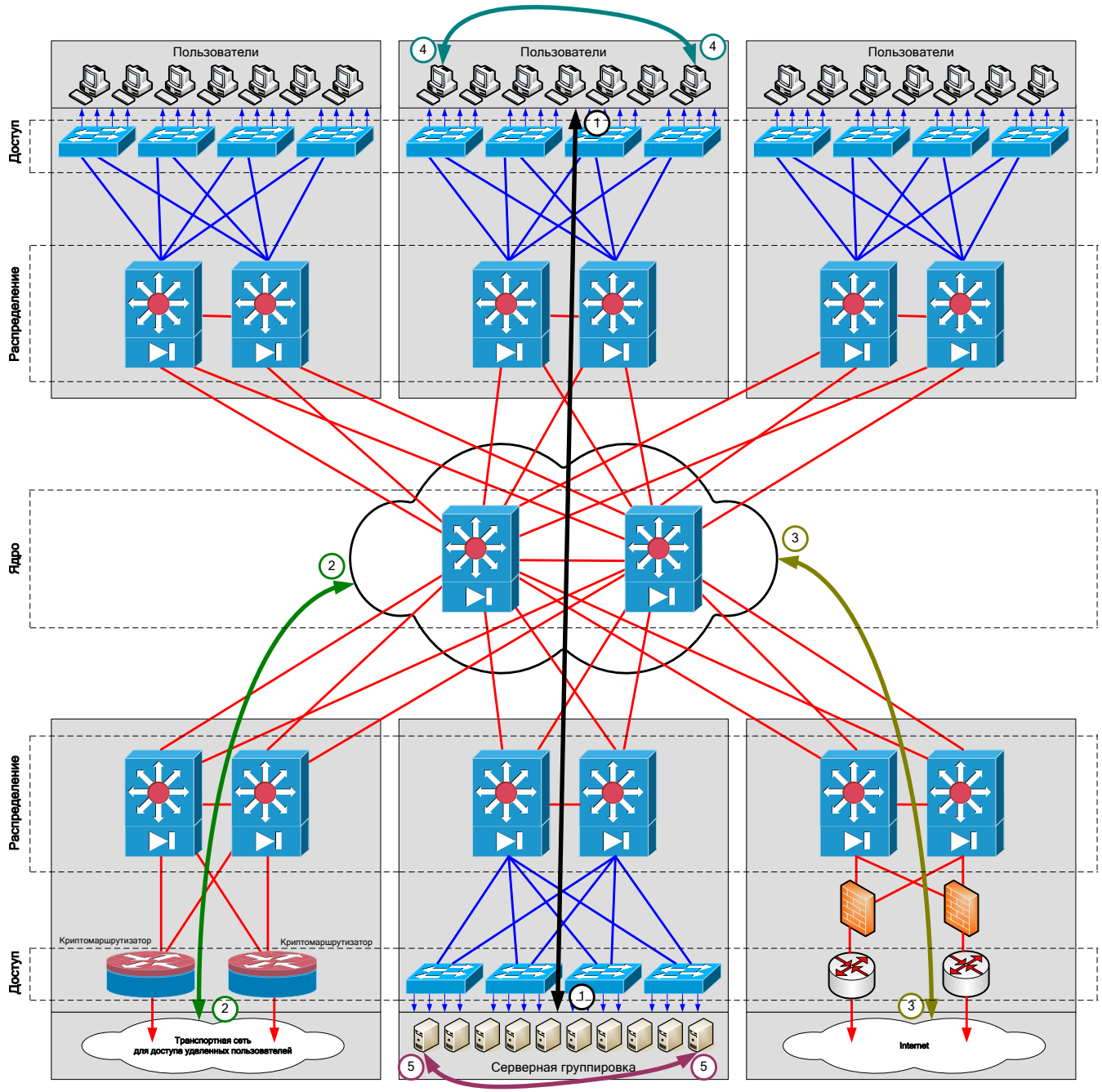

Рисунок 2.3 – Информационные потоки корпоративной сети, построенной на основе трехуровневой модели

2.3.12 Таким образом, при выборе мест установки сетевых датчиков, целесообразно защищать периметр сети – контролировать на наличие компьютерных атак следующие информационные потоки:

– информационный поток между удаленными пользователями и корпоративной сетью (поток № 2) – для защиты от нарушителей, которые могут находиться на удаленных рабочих местах (точка включения сетевого приведена на рисунке 2.3);

– информационный поток между корпоративной сетью и, ресурсами и пользователями, находящимися в открытых сетях передачи данных, таких как сеть Internet (поток № 3) – для защиты от нарушителей, не являющихся пользователями корпоративной сети (точки включения сетевых датчиков приведены на рисунке 2.4).

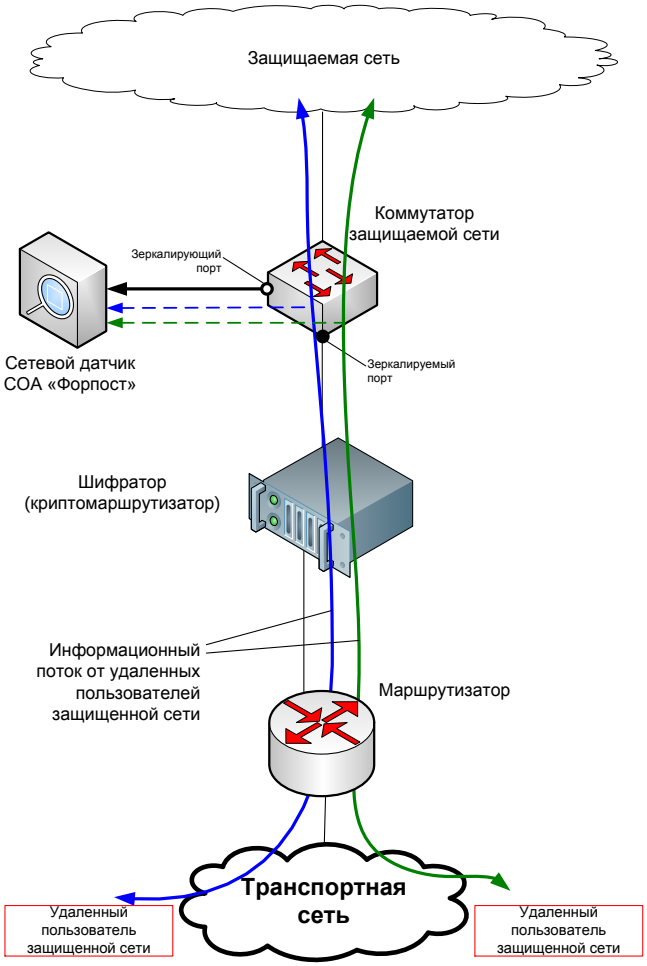

Рисунок 2.3 – Схема включения СОА «Форпост» на границе сети для защиты от внутреннего нарушителя

2.3.13 На рисунке 2.3 показана защищаемая сеть, подключенная к некой транспортной сети (например, к сети Internet) только для обеспечения транспорта зашифрованного трафика. Функции основной защиты от внешних нарушителей выполняет криптомаршрутизатор, который изолирует защищаемую сеть от открытой транспортной сети передачи данных.

В этом случае СОА «Форпост» применяется для защиты информационных ресурсов защищаемой сети от внутренних нарушителей. Внутренние нарушители могут, например, находиться на удаленных объектах защищаемой сети (которые администратору, как правило, слабо подконтрольны) и могут несанкционированно реализовывать компьютерные атаки на информационные ресурсы (сервера приложений, базы данных и пр.).

Информационные потоки от внешних абонентов к ресурсам защищаемой сети условно показаны на схеме непрерывными кривыми линиями. Предлагается проводить анализ информации в этих информационных потоках на предмет наличия в них признаков компьютерных атак, подавая копии этих информационных потоков (они на участке между криптомаршрутизатором и коммутатором защищаемой сети не зашифрованы) на сетевой датчик СОА «Форпост» (пунктирные линии на рисунке 2.3).

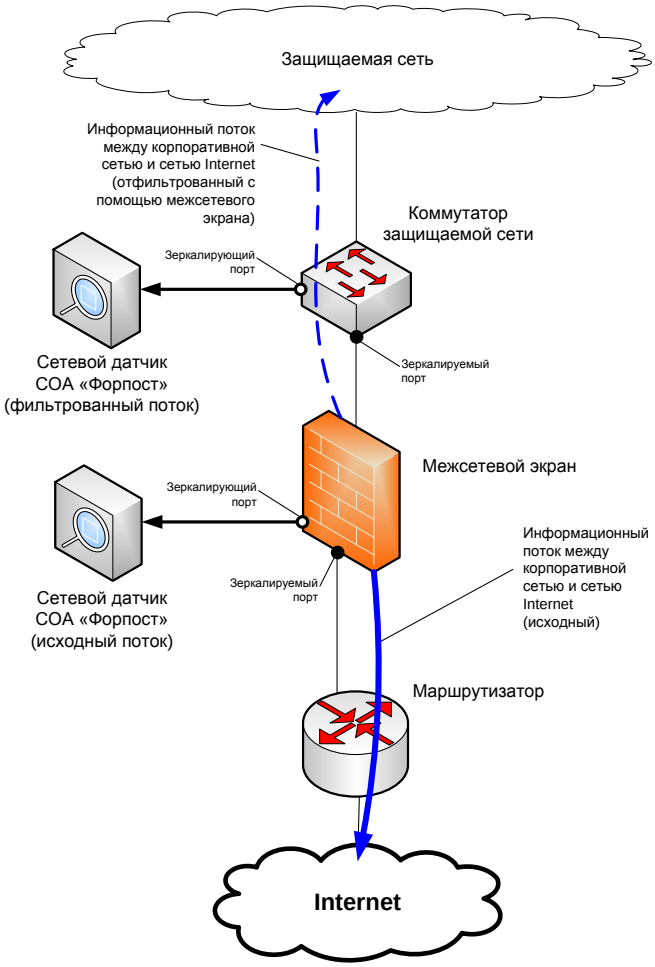

Рисунок 2.4 – Схема включения СОА «Форпост» на границе сети для защиты от внешнего нарушителя

2.3.14 В случае наличия межсетевого экрана (рисунок 2.4) трафик можно снимать:

- до межсетевого экрана (со стороны сети Internet);
- после межсетевого экрана (со стороны защищаемой сети);
- в обоих точках одновременно.

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 опубли-

кованных для доступа из сети Internet, то месторасположение сетевого датчика не имеет значение. Однако, следует отметить, что:

− установка датчика до межсетевого экрана (со стороны сети Internet) 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 защищаемой сети) 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).

2.3.15 Так же необходимо подвергать мониторингу на наличие компьютерных атак информационный поток между серверами и локальными пользователями (поток № 1) – для защиты от нарушителей, являющихся пользователями сети (если пользователи сети не являются нарушителями – то для защиты от их нецеленаправленных, случайных действий, которые могут повлиять на безопасность корпоративной сети). Единым устройством сети, в которое сходится указанный информационный поток является ядровой коммутатор (рисунок 2.2). Однако суммарный объем трафика, который несет в себе данный информационный поток может значительно превышать пропускную способность имеющихся зеркалирующих портов коммутатора, а так же возжможности сетевого датчика. В связи с этим, необходимо анализировать объем трафика и при большом его количестве в качестве точек подключения выбирать коммутаторы уровня распределения или коммутаторы уровня доступа.

2.3.16 Дополнительно, с целью более детального анализа поведения нарушителя можно контролировать информационный поток между серверами (поток № 5). Это может быть полезно, когда нарушитель применяет тактику взлома одного инфорамционного ресурса, а все свои последующие действия в сегменте серверов выполяет уже с этого взломанного ресурса. В этом случае контроля лишь одного периметра сети (потоки № 2 и 3) и информационного потока между серверами и пользователями (поток № 1) может оказаться недостаточно. В качестве точки съема трафика рекомендуется выбирать коммутаторы уровня доступа. В зависимости специфики информационных ресурсов, находящихся на серверах, и объемов трафика, которые они генерируют, выбирается количество подключаемых сетевых датчиков. Рекомендуемое максимальное количество серверов для сетевого датчика с производительностью до 1 Гбит/с – до 5-10 штук.

2.3.17 Компьютеры пользователей не содержат информационных ресурсов, однако могут содержать информацию, конфиденциальность, целостность или доступность которой может быть критична для конкретного пользователя. В этом случае целесообразно контролировать информа-

ционный поток между локальными пользователями (поток № 1). В качестве точки съема трафика рекомендуется выбирать коммутаторы уровня доступа. Рекомендуемое максимальное количество компьютеров пользователей для сетевого датчика с производительностью до 1 Гбит/с – до 20-30 штук.

2.3.18 В случае, когда в сети 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.

2.3.19 При настройке зеркалирующих портов (SPAN) необходимо учитывать следующие технологии, обычно используемые в корпоративных сетях:

− EtherChannel (агрегация каналов) – на сетевой датчик должен поступать трафик со всех каналов; при использовании данной технологии SPAN-порт необходимо настраивать на виртуальный EtherChannel-интерфейс, а не отдельные физические интерфейсы

− VLAN по стандарту IEEE 802.1Q – направление на сетевой датчик трафика от нескольких VLAN нежелательно, т к. возможно пересечение разнородных информационных потоков, в том числе по IP-адресам, однако возможно при условии настройки сетевого датчика, оборудования, зеркалирующего трафик, и оборудования, на котором установлен сетевой датчик на передачу метки, содержащий номер VLAN (в этом случае номер VLAN, в котором обнаружена атака будет отображаться в журнале СОА);

− STP (Spanning Tree Protocol) – при использовании данного протокола для работы режима резервирования активного сетевого оборудования необходимо отслеживать, что сетевой датчик подключен к активному порту.

2.4 О режимах работы сетевого датчика (Half Duplex, Full Duplex)

2.4.1 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 сервера 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 2 зеркалирующих сетевых интерфейсов со скоростью 1 Гбит/с.

2.4.2 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 2.4 «а)»»;

– 1 зеркалирующий сетевой интерфейс 10 Гбит/с – рисунок 2.4 «б)».

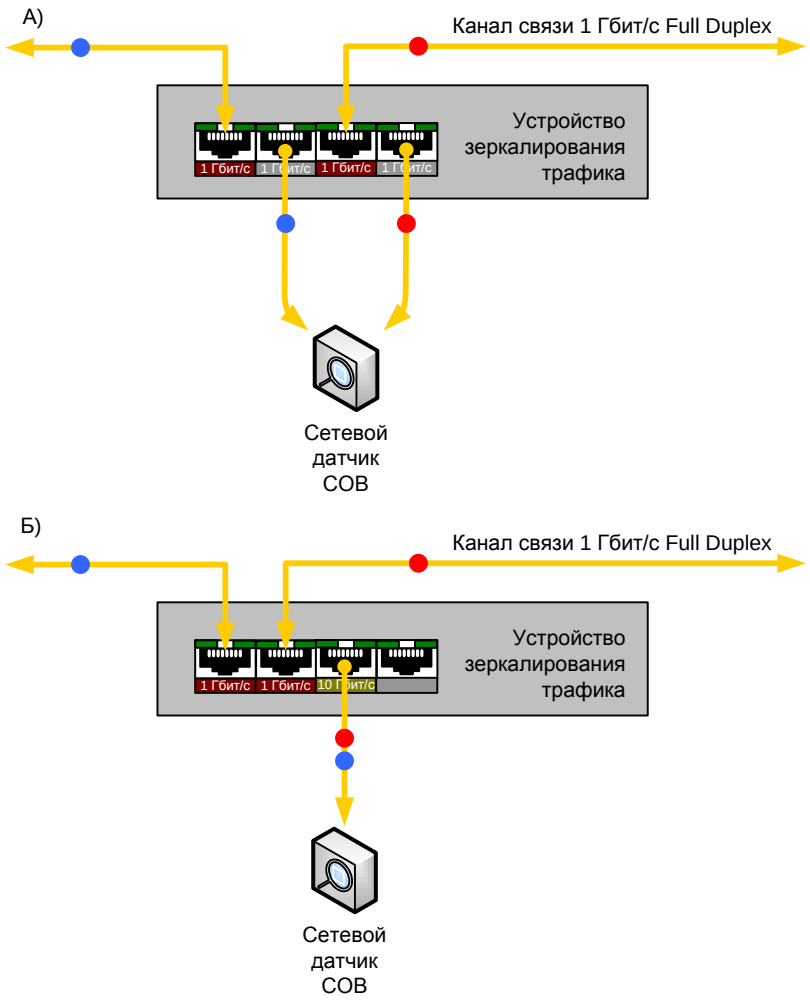

Рисунок 2.4 – Обеспечение съёма сетевого трафика в режиме Full Duplex:

а) при использовании двух сетевых портов

б) при использовании сетевого порта большей производительности.

2.4.3 Использовать зеркалирующий порт с меньшей пропускной способностью можно, если прогнозируемый объем трафика не превысит пропускную способность зеркалирующего порта коммутатора, но при этом следует учитывать, что в случае всплесков сетевой активности часть трафика все таки не будет попадать на сетевой датчик для анализа.

2.4.4 Поддержка режиме Full Duplex присутствует в сетевом датчике СОА «Форпост» версии 0.2.

2.4.5 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).

2.5 Проектирование конфигурации аппаратного обеспечения СОА

2.5.1 Минимальные системные требования

2.5.1.1 СОА «Форпост» предъявляет следующие минимальные системные требования:

- операционная система Windows Server 2003/2008/2012/XP/7/8;
- процессор с частотой не менее 1,6 ГГц;
- оперативной памяти не менее 2 ГБ;
- объем свободного дискового пространства не менее 20 ГБ;
- сетевой интерфейс со скоростью не менее 100 Мбит/с;
- на сервере с сетевым датчиком – дополнительно не менее 1 сетевого интерфейса для захвата трафика со скоростью не менее 100 Мбит/с, предпочтительно, в серверном исполнении.

2.5.1.2 Поскольку система распределенная, компоненты СОА могут быть установлены как на один сервер, так и распределены на несколько физических серверов.

2.5.1.3 При повышенных требованиях по производительности рекомендуется:

- на серверах с информационным фондом, координационными центрами, сетевыми датчиками увеличить тактовую частоту процессора и использовать многоядерные, либо многопроцессорные конфигурации; использовать серверные версии операционной системы Windows;
- на серверах с сетевыми датчиками увеличить объем оперативной памяти до 16 ГБ;
- привести объем дискового пространства в соответствие с потребностями информационного фонда по объему единовременно хранимой в системе информации о событиях;
- на серверах с сетевыми датчиками для захвата трафика использовать сетевые интерфейсы со скоростью 1 или 10 Гбит/с в серверном исполнении.

2.5.2 Сетевой датчик

2.5.3 Для того, что бы сетевой датчик мог обрабатывать поток трафика со скоростью:

- до 100 Мбит/с, число процессорных ядер должно быть не менее 1 шт.;
- до 500 Мбит/с – не менее 4 шт.;
- до 1 Гбит/с Half Duplex или 2 Гбит/с Full Duplex – не менее 8 шт.;
- до 2 Гбит/с Half Duplex или 4 Гбит/с Full Duplex – не менее 16 шт.

2.5.4 На сервере с сетевым датчиком технология Hyper-Threading должна быть отключена.

2.5.5 На сервере с сетевым датчиком должны быть установлены:

- для передачи данных к другим компонентам СОА – один сетевой интерфейс;
- для съема трафика сетевым датчиком в режиме Half Duplex – один сетевой интерфейс, в режиме Full Duplex – два сетевых интерфейса.

2.5.6 Информационный фонд

2.5.6.1 ПО информационного фонда устанавливается на сервера с установленной СУБД MS SQL 2005/2008/2012/2014. Конкретные системные требования для работы ПО информационного фонда определяются системными требованиями СУБД MS SQL 2005/2008/2012/2014 и зависят от предполагаемой нагрузки на СОА «Форпост».

2.5.6.2 Необходимо быть уверенным в достаточности объема дискового пространства в соответствие с потребностями информационного фонда по объему единовременно хранимой в системе информации о событиях.

2.5.7 Координационный центр

2.5.7.1 Производительность сервера для координационного центра зависит от объема информации, которая должна единовременно передаваться от датчиков в информационный фонд. Если требуется передавать информацию от нескольких датчиков со скоростью более 500 сообщений в секунду, рекомендуется использовать многоядерные серверы.

2.5.7.2 Для работы в режиме резервирования требуется не менее двух серверов.

2.5.7.3 Дополнительных специальных требований не предъявляется.

2.5.8 Консоль администратора

2.5.8.1 Консоль администратора как правило устанавливается на АРМ администратора безопасности.

2.5.8.2 Дополнительных специальных требований не предъявляется.

2.5.9 Прочие компоненты

2.5.9.1 Агент управления и датчик контроля целостности устанавливаются совместно с другими компонентами СОА «Форпост». Специальных системных требований не предъявляют, однако следует учитывать, что при контроле целостности ресурсов датчики контроля целостности, в зависимости от количества установленных на контроль ресурсов, производят отъем части системных ресурсов у защищаемого узла.

2.5.9.2 Модуль почтовых уведомлений, модуль интеграции с сетевым оборудованием специальных системных требований не предъявляют.

2.6 Правила обращения с криптографическими ключами

2.6.1 Правила обращения с криптографическими ключами, перечисленные ниже могут дополняться требованиями к АИС, в которую встраивается СОА; требованиями используемой СКЗИ (для СКЗИ КриптоПро 3.6 данные требования определены в документе «Руководство администратора безопасности. Общая часть», ЖТЯИ.00050-02 90 02; для СКЗИ КриптоПро 3.6.1 данные требования определены в документе «Руководство администратора безопасности. Общая часть», ЖТЯИ.00050-03 90 02).

2.6.2 Перечень возможных ключевых носителей зависит от типа используемого СКЗИ (для СКЗИ КриптоПро 3.6 данные требования определены в документе «Руководство администратора безопасности. Общая часть», ЖТЯИ.00050-02 90 02; для СКЗИ КриптоПро 3.6.1 данные требования определены в документе «Руководство администратора безопасности. Общая часть», ЖТЯИ.00050-03 90 02), требованиями к АИС, в которую встраивается СОА. Ключевой носитель для хранения закрытого ключа, используемого для подписывания файла, содержащего список контролируемых на целостность ресурсов, должен быть отчуждаемым.

2.6.3 При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Администратор безопасности и пользователь несет персональную ответственность за хранение личных ключевых носителей.

2.6.4 Конкретный перечень правил должен быть определен исходя из условий эксплуатации СКЗИ.

2.7 Организационно-технические мероприятия по защите от несанкционированного доступа (НСД)

2.7.1 Организационно-технические мероприятия по защите от НСД, перечисленные ниже, могут дополняться требованиями к АИС, в которую встраивается СОА; требованиями используемой СКЗИ (для СКЗИ КриптоПро 3.6 данные требования определены в документе «Руковод-

ство администратора безопасности. Общая часть», ЖТЯИ.00050-02 90 02; для СКЗИ КриптоПро 3.6.1 данные требования определены в документе «Руководство администратора безопасности. Общая часть», ЖТЯИ.00050-03 90 02).

2.7.2 При использовании СКЗИ должны выполняться следующие меры по защите информации от НСД:

- Необходимо разработать и применить политику назначения и смены паролей.
- Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.
- Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

2.7.3 Запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным; выводить ключевую информацию на дисплей, принтер и т. п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию.

2.7.4 Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии ОС;
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;
- на ПЭВМ должна быть установлена только одна операционная система;
- правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;

− должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;

− необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;

− в случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети;

− при использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN сетей и т.п.); при этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации;

− организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

− организовать и использовать комплекс мероприятий антивирусной защиты.

Рекомендуется аппаратуру, на которой устанавливается СКЗИ, проверить на отсутствие аппаратных закладок.

2.7.5 Не допускается:

1) Осуществлять несанкционированное копирование ключевых носителей.

2) Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).

3) Вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.

4) Подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.

5) Работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ.

6) Вносить какие-либо изменения в программное обеспечение СКЗИ.

7) Изменять настройки, установленные программой установки СКЗИ или администратором.

2.7.6 Конкретный перечень организационно-технические мероприятия по защите от НСД должен быть определен исходя из условий эксплуатации СКЗИ.

3 ОПИСАНИЕ ЗАДАЧ, РЕШАЕМЫХ СОА И МЕТОДОВ ИХ РЕШЕНИЯ

3.1 Система обнаружения атак – это система, целевая функция которой заключается в автоматическом выявлении воздействий на контролируемую данной системой АИС, которые могут быть классифицированы как компьютерные атаки.

3.2 Существует три метода выявления компьютерных атак, реализуемых в СОА:

- метод, основанный на использовании базы данных сигнатур атак, где сигнатура атаки – это структура данных специального вида или шаблон, описывающие состояние АИС, классифицируемое как компьютерная атака;
- метод, основанный на накоплении и анализе знаний о контролируемой системе
- комбинирование указанных методов.

3.3 В основу функционирования сетевого датчика СОА «Форпост» положен сигнатурный метод выявления атак. Он обеспечивает обнаружение атак на основе специальных шаблонов (сигнатур), каждый из которых соответствует конкретной атаке. При получении исходных данных о сетевом трафике информационной системы, СОА «Форпост» производит их анализ на соответствие указанным шаблонам атак, имеющихся в базе данных.

В случае обнаружения сигнатуры в исходных данных, система регистрирует факт обнаружения атаки, оповещает администратора безопасности о данном событии и предоставляет возможность администратору произвести блокирование источника атаки с помощью соответствующего коммуникационного оборудования.

За счет использования датчиков контроля целостности СОА позволяет отслеживать действия нарушителя по отношению к контролируемым ресурсам в скомпрометированной системе.

Дополнительно поддерживается получение данных о функционировании отдельных объектов контролируемой АИС по протоколам syslog и SNMP.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Входные данные

Входными данными системы является трафик, передающийся в контролируемой системе, отслеживаемый датчиками, а также конфигурационная информация, задаваемая администратором системы при ее настройке.

4.2 Выходные данные

Выходными данными является информация, сгенерированная компонентами об обнаруженных компьютерных атака и других событиях, произошедших.