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

СОВ ПАК «Плутон»

Описание функциональных характеристик программного обеспечения

Листов 22

2016

Содержание

# 1 ВВЕДЕНИЕ

Представляемый в данном документе материал описывает функциональные характеристика программного обеспечения Системы обнаружения вторжений программно-аппаратный комплекс СОВ ПАК «Плутон».

# 2 СОСТАВ СОВ ПАК «ПЛУТОН»

## 2.1 Общие сведения

Анализ сетевого трафика – это комплекс организационных мер и программно-технических средств используемых для сбора, хранения и обработки получаемой из сети информации.

Несанкционированные действия определяются как компьютерные атаки (КА), направленные на контролируемую сеть.

СОВ ПАК «Плутон» обеспечивает анализ сетевого трафика на наличие сетевых вторжений и аномалий поведения на каналах связи с пропускной способностью не менее 1 Гбит/с или 10 Гбит/с (зависит от комплектации).

В комплекс входят программные и технические средства, обеспечивающие функционирование ПАК, а также комплект эксплуатационных и технических документов.

СОВ ПАК «Плутон» включает:

– средства обнаружения компьютерных атак (КА);

– средства анализа информации о КА;

– долговременное хранилище данных;

– средства визуального отображения результатов работы системы;

– средства управления системой;

– защищенные средства связи между компонентами системы.

## 2.2 Состав и назначение программного обеспечения

Система обнаружения вторжений программно-аппаратный комплекс (далее – СОВ ПАК «Плутон» или Изделие) включает в себя:

1) Программное обеспечение (далее – ПО) – программное средство (далее – ПС) сенсор регистрации сетевых вторжений в 4 вариантах исполнения (далее – ПС «Сенсор»).
2) ПО – ПС «Сервер УС».
3) ПО – ПС «АРМ УС».

4) ПО – криптографическая защита канала управления и передачи данных о выявленных сетевых вторжениях (далее – ПС «СКЗИ канала управления»).
5) Общесистемное программное обеспечение (далее – ОПО) – операционная система (далее ОПО ОС).
6) ОПО система управления базами данных (СУБД).

2.2.1 Функции ПС «Сенсор»

ПС «Сенсор» фиксирует первичную информацию о сетевых вторжениях и событиях безопасности (далее – событиях) в контролируемых системах. При этом все сенсоры, подключенные к ПС «Сервер УС», имеют уникальный идентификатор (далее – УИ).

ПС «Сенсор» функционирует в однопользовательском режиме и обеспечивает замкнутую программную и командную среду.

ПС «Сенсор» реализует замкнутую программную командную среду методом применения согласованного списка команд и специальной командной оболочки, как для сетевых, так и для локальных подключений администратора безопасности СОВ. При этом сохраняется технологическая роль суперпользователя, доступная при вводе пароля локально.

ПС «Сенсор» реализует функции работы отказоустойчивого кластера, по признакам работоспособности узла и канала передачи данных.

ПС «Сенсор» маскирует факт собственной работы, функционируя только в режиме прослушивания тракта передачи данных.

ПС «Сенсор» регистрирует и идентифицирует события сетевых вторжений в каналах передачи данных (далее – каналы) на основе анализа сетевого трафика, передаваемого по каналам связи с использованием протоколов IPv4.

ПС «Сенсор» имеет возможность анализа сетевого трафика на наличие компьютерных атак на каналах связи с пропускной способностью не менее 1 Гбит/с, 10 Гбит/с (зависит от комплектации).

ПС «Сенсор» в качестве механизмов анализа использует сигнатурный и статистический методы поиска сетевых вторжений.

Сигнатурный метод анализа основан на возможности применения базы решающих правил системы обнаружения атак `Snort`. С его помощью определяется не менее 10 000 компьютерных вторжений в секунду, при этом вероятность возникновения ошибки первого рода не превышает 5%, а ошибки второго рода 2%.

Статистический метод анализа строится на основе возможности передачи данных о количественных характеристиках сетевого трафика, проходящего через обслуживаемый канал связи за единицу времени по протоколу NetFlow на ПС «Сервер УС» для работающего статистического анализатора.

ПС «Сенсор» хранит базу решающих правил сигнатурного анализа, на основании которых регистрируются сетевые вторжения.

ПС «Сенсор» обладает возможностью получения, изменения и удаления данных из базы решающих правил с ПС «АРМ УС» от имени учетной записи администратора безопасности СОВ.

ПС «Сенсор» обеспечивает обработку, фрагментированного сетевого трафика, GRE-туннелей, любых комбинаций инкапсуляции протоколов IPv4 и IPv6.

Управление настройками и состоянием ПС «Сенсор» осуществляется только от имени учетной записи администратора безопасности СОВ с ПС «АРМ УС».

ПС «Сенсор» просматривает сетевой трафик на предмет обнаружения подозрительных событий и сетевых вторжений, при обнаружении которых фиксируются следующие параметры:

а) код регистрируемого события или вторжения;

б) дата и время события или вторжения;

в) идентификатор источника события или атаки (если такой существует и его можно определить на основе анализа сетевого трафика);

г) сетевой адрес источника сетевого вторжения;

д) аппаратный адрес из состава кадра, содержащего сетевое вторжение;

е) подозрительный пакет данных (настраиваемый параметр);

ж) идентификатор несоответствия протокола RFC (настраиваемый параметр);

з) идентификаторы мандатных уровней и категорий, передающиеся в составе IP пакета данных для ОС;

и) идентификатор узла, в отношении которого производиться данное событие или вторжение (если такой существует и его можно определить на основе анализа сетевого трафика);

к) используемый протокол сетевого уровня;

л) номер порта протокола сетевого уровня.

ПС «Сенсор» передает информацию (событие информационной безопасности (далее – СИБ)) обо всех событиях, выявленных в контролируемом канале с указанием УИ сенсора.

ПС «Сенсор» обеспечивает гарантированную доставку СИБ от сенсора к ПС «Сервер УС».

ПС «Сенсор» накапливает информацию обо всех выявленных сетевых вторжениях в автономном режиме (до восьми часов работы) и передает их в ПС «Сервер УС» при восстановлении связи.

ПС «Сенсор» накапливает статистическую информацию о работе сети в автономном режиме и передает их в ПС «Сервер УС» при восстановлении связи. Величина счетчиков достаточна для хранения данных о работе сети на период до восьми часов.

При переполнении данных счетчиков статистического анализатора они сбрасываются. По результатам сброса статистических счетчиков формируется специальный СИБ, который отсылается на ПС «Сервер УС» в момент восстановления соединения.

ПС «Сенсор» при увеличении времени автономной работы использует механизм циклической записи информации о возникающих сетевых вторжениях. В случае срабатывания механизма циклической записи (обнуление событий)

формируется специальный СИБ, который отсылается на ПС «Сервер УС» в момент восстановления соединения.

ПС «Сенсор» имеет функции контроля целостности своего программного обеспечения (далее – ПО), конфигурационных файлов, базы решающих правил сигнатурного анализа:

а) при старте ПО;

б) по установленным временным интервалам;

в) по команде администратора безопасности и оператора визуального контроля СОВ с ПС «АРМ УС».

ПС «Сенсор» имеет механизмы самотестирования работы: передачи данных для статистического анализа, сигнатурного анализатора, функций журналирования событий, авторизации администратора СОВ, контроля целостности и передачи СИБ:

а) при старте ПО;

б) по установленным временным интервалам;

в) по команде администратора безопасности и оператора визуального контроля СОВ с ПС «АРМ УС».

ПС «Сенсор» формирует СИБ через период времени, задаваемый оператором. СИБ содержит следующую информацию:

а) целостность программного обеспечения;

б) целостность конфигурационных файлов;

в) целостность используемой базы правил сигнатурного анализа;

г) результаты прохождения последнего самотестирования;

д) проценте загрузки системной памяти;

е) время работы системы относительно последней перезагрузки;

ж) процент заполнения НЖМД.

ПС «Сенсор» выполняет журналирование следующих событий:

а) запуск и остановка ОПО ОС;

б) выполнение функций по локальному или удаленному доступу;

в) запуск и останов процессов сигнатурного и статистического анализаторов;

г) чтение данных журналирования событий;

д) передача данных события безопасности на ПС «АРМ УС»;

е) попытки удаления файлов журналов безопасности;

ж) модификация и настройка функции анализа сетевых вторжений и журналирования событий;

з) изменение состояния элементов кластера;

и) изменение системного времени;

к) результаты самотестирования.

ПС «Сенсор» связывает каждое событие журнала безопасности под наименованием учетной записи администратора безопасности ПС «АРМ УС»;

а) с датой и временем возникновения события;

б) с идентификатором процесса события;

в) с результатами выполнения.

ПС «Сенсор» обладает возможностью экспорта журнала аудита безопасности на ПС «АРМ УС» по команде администратора безопасности. Каждый журнал сопровождается его контрольной суммой.

По результатам экспорта существующие журналы удаляются, а первой записью нового журнала ПС «Сенсор» становится запись об его отчуждении с указанием его контрольной суммы.

### 2.2.3 Функции ПС «Сервер УС»

ПС «Сервер УС» функционирует в однопользовательском режиме и обеспечивает замкнутую программную и командную среду.

ПС «Сенсор» реализует замкнутую программную командную среду, методом применения согласованного списка команд и специальной командной оболочки, как для сетевых, так и для локальных подключений администратора безопасности СОВ, сохраняя технологическую роль суперпользователя, доступную при вводе пароля локально.

ПС «Сервер УС» опрашивает, принимает и обрабатывает поступающие от сенсоров СИБ и снабжает их следующей сопроводительной информацией:

а) приоритет сообщения – числовой параметр принимающий значение от 0 до 4;

б) флаг критичности сообщения (необходимость немедленного оповещения оператора ПС «АРМ УС»).

ПС «Сервер УС» автоматически определяет доступность и работоспособность ПС «Сенсор».

ПС «Сервер УС» сохраняет данные СИБ о выявленных сетевых вторжениях в базе данных сетевых вторжений на ОПО СУБД в течении минимум двух лет с момента его возникновения.

ПС «Сервер УС» обеспечивает запись СИБ в базу данных сетевых вторжений с производительностью не менее 40 000 записей в секунду.

ПС «Сервер УС» обеспечивает функции автоматизированного (по команде администратора безопасности СОВ) архивирования и очистки данных о СИБ, возникших более двух лет назад с текущей даты функционирования.

ПС «Сервер УС» сохраняет данные о СИБ в архиве до пяти лет.

ПС «Сервер УС» обеспечивает автоматизированное (по команде оператора) восстановление данных из архива СИБ, для выполнения поиска данных посредством ПС «АРМ УС».

ПС «Сервер УС» выполняет поиск СИБ в ОПО СУБД по сложным вложенным запросам, передающимся с ПС «АРМ УС», для обеспечения визуализации статистик сетевых вторжений, субъектов и объектов угроз и др.

ПС «Сервер УС» обеспечивает поиск данных СИБ в ОПО СУБД с произвольностью не менее 60 000 записей в секунду.

ПС «Сервер УС» формирует СИБ для отправки на ПС «АРМ УС» с установленным флагом критичности при пропадании связи с любым из обслуживаемых сенсоров.

ПС «Сервер УС» формирует СИБ об изменении состояния элементов кластера сенсоров.

ПС «Сервер УС» обеспечивает данными из базы данных сетевых вторжений систему управления событиями безопасности (SIEM-система), функционирующую на ПС «АРМ УС».

ПС «Сервер УС» содержит в локальной базе данных базу приоритетов сетевых вторжений.

ПС «Сервер УС» идентифицирует атаки путем сравнения идентификатора сообщений, поступающих от сенсоров с идентификаторами, хранящимися в базе данных сетевых вторжений.

ПС «Сервер УС» выявляет наиболее активные источники сетевых вторжений и записывает информации по ним в соответствующие таблицы базы данных сетевых вторжений.

ПС «Сервер УС» хранит базу решающих правил сигнатурного анализа и статистических профилей.

ПС «Сервер УС» позволяет редактировать базы решающих правил сигнатурного анализа администратору безопасности СОВ.

ПС «Сервер УС» осуществляет централизованную рассылку и применение правил сигнатурного анализа сетевых вторжений по команде администратора безопасности СОВ.

ПС «Сервер УС» выполняет функции статистического анализатора – оценивает результаты текущих выборок сетевой активности, получаемых с ПС «Сенсор» по отношению к статистикам, накопленным за период обучения:

а) статистический метод анализа основан на оценке расхождения накопленных результатов реализаций статистических выборок (количественных характеристик по пакетам протоколов с уже установленными соединениями и числа попыток установления соединения) с текущими показателями сетевой активности по общепринятым или неизвестным протоколам связи, использующим неизвестные серверные порты;

б) статистический метод анализа использует в своей работе период обучения, не превышающий 48 часовой интервал времени работы;

в) статистический метод имеет функцию настройки политики применения критериев расхождения реализаций выборок, задаваемых в количественных характеристиках: количество пакетов в единицу времени в рамках установленных соединений или вновь открываемых соединений в интервал времени, задаваемый администратором безопасности СОВ.

ПС «Сервер УС» позволяет администратору безопасности СОВ группировать статистические правила как для отдельных сенсоров, так и для групп сенсоров.

ПС «Сервер УС» хранит настройки статистических критериев для подключенных сенсоров, групп сенсоров.

ПС «Сервер УС» предоставляет пользователю с правами администратора безопасности СОВ следующие функции управления:

а) ввод нового обслуживаемого ПС «Сенсор»;

б) управление состоянием ПС «Сервер УС»;

в) управление таблицами базы данных сетевых вторжений;

г) управление таблицами базы данных управления межсетевыми экранами;

д) изменение настроек конфигурационных файлов;

е) настройка функций автоматического применения правил межсетевого экранирования;

ж) выполнение задач по автоматизированному применению правил межсетевого экранирования;

з) управление правилами сигнатурного анализа;

и) управление профилями и задание граничных значений статистического анализатора.

ПС «Сервер УС» поддерживает иерархическую модель подчинения:

а) передавая (получая) на вышестоящий (с нижестоящего) в иерархии ПС «Сервер УС» данные о сетевых вторжениях;

б) передавая (получая) на вышестоящий (с нижестоящего) в иерархии ПС «Сервер УС» данные о выявленных статистическим анализатором сетевых аномалиях.

ПС «Сервер УС» контролирует целостность своего ПО и конфигурационных файлов:

а) при старте ПО;

б) по установленным временным интервалам;

в) по команде администратора безопасности и оператора визуального контроля СОВ с ПС «АРМ УС».

ПС «Сервер УС» имеет механизмы самотестирования работы сигнатурного анализатора, функции журналирования событий, авторизации администратора СОВ, контроля целостности и получения СИБ:

а) при старте изделия;

б) по установленным временным интервалам;

в) по команде администратора безопасности и оператора визуального контроля СОВ с ПС «АРМ УС».

По результатам выполнения функций самотестирования и контроля целостности ПС «Сервер УС» отравляет СИБ на ПС «АРМ УС» с указанием результата.

Доступ к управлению состоянием ПС «Сервер УС», изменению файлов конфигурации и граничных значений имеют только администраторы безопасности СОВ ПС «АРМ УС».

ПС «Сервер УС» журналирует события в части:

а) локального и удаленного доступа к изделию;

б) запуска и останова процессов ПС «Сервер УС», ОПО СУБД;

в) чтения данных журналирования событий;

г) попыток удаления данных журналирования событий;

д) передачи данных аудита на ПС «АРМ УС»;

е) модификации и настройки функции регистрации сетевых вторжений и аудита событий;

ж) изменения состояний базы решающих правил сигнатурного анализа;

з) изменения базы решающих правил на сенсорах, группах сенсоров;

и) изменения статистических критериев оценки событий в обслуживаемой сети;

к) изменения системного времени;

л) получения результатов самотестирования.

ПС «Сервер УС» связывает каждое событие аудита безопасности под наименованием учетной записи администратора безопасности СОВ ПС «АРМ УС»;

а) с датой и временем возникновения события;

б) с идентификатором процесса события;

в) с результатом выполнения.

ПС «Сервер УС» обладает возможностью экспорта журналов аудита безопасности на ПС «АРМ УС» только по команде администратора безопасности СОВ. Каждый журнал сопровождается его контрольной суммой.

По результатам экспорта текущие журналы удаляются, а первой записью нового журнала ПС «Сервер УС» становится запись об его отчуждении с указанием его контрольной суммы.

### 2.2.5 Функции ПС «АРМ УС»

ПС «АРМ УС» функционирует в однопользовательском режиме.

ПС «АРМ УС» предоставляет администратору безопасности и оператору визуального контроля СОВ для работы графический оконный интерфейс.

ПС «АРМ УС» функционирует в рамках ролевой модели управления.

ПС «АРМ УС» поддерживает следующие роли:

а) администратор безопасности СОВ;

б) оператор визуального контроля СОВ.

Роль оператора визуального контроля СОВ в ПС «АРМ УС» предназначена для выполнения функций мониторинга:

а) сетевых вторжений;

б) критических событий;

в) применения правил межсетевого экранирования;

г) состояния работоспособности обслуживаемых сенсоров и сервера управления сенсорами.

Роль оператора визуального контроля СОВ ПС «АРМ УС» позволяет:

а) управлять автоматизированной отправкой созданного на ПС «Сервер УС» правила межсетевого экранирования на межсетевой экран;

б) выполнять команды самотестирования ПС «Сенсор», ПС «Сервер УС» и ПС «АРМ УС».

Роль администратора безопасности СОВ ПС «АРМ УС» предназначена для выполнения функций мониторинга и аудита:

а) сетевых вторжений;

б) критических событий;

в) применения правил межсетевого экранирования;

г) состояния работоспособности обслуживаемых сенсоров и сервера управления сенсорами;

д) событий безопасности ПС «Сенсор», ПС «Сервер УС» и ПС «АРМ УС».

Роль администратора безопасности СОВ ПС «АРМ УС» предназначена для управления:

а) запуском и остановом ПС «Сенсор»;

б) конфигурацией ПС «Сенсор»;

в) вводом новых ПС «Сенсор» в обслуживание на ПС «Сервер УС»;

г) получением данных журналирования событий с ПС «Сенсор»;

д) получением данных журналирования событий с ПС «Сервер УС»;

е) аудитом событий ПС «АРМ УС», ПС «Сенсор» и ПС «Сервер УС»;

ж) базой решающих правил сигнатурного анализа для применения на ПС «Сенсор»;

з) статистическими профилями и критериями для применения в статистическом анализе на ПС «Сервер УС»;

к) базой данных сетевых вторжений, загрузкой архивных СИБ;

л) базой данных правил межсетевого экранирования;

м) базой данных статистических профилей и правил сигнатурного анализа;

н) командами самотестирования ПС «Сенсор» и ПС «Сервер УС».

ПС «УС» позволяет администратору безопасности СОВ устанавливать порядок и периодичность опроса сенсоров.

ПС «АРМ УС» позволяет администратору безопасности СОВ устанавливать для СИБ сопроводительную информацию и правила их распределения.

ПС «АРМ УС» позволяет администратору безопасности СОВ управлять архивированием и восстановлением баз данных сетевых вторжений.

ПС «АРМ УС» позволяет администратору безопасности СОВ осуществлять администрирование базы данных сетевых вторжений.

ПС «АРМ УС» дает возможность администратору безопасности СОВ настраивать профили статистического анализатора на ПС «Сервер УС».

ПС «АРМ УС» предоставляет администратору безопасности СОВ возможность автоматизировано обновлять базу решающих правил на группе сенсоров, либо на единичном сенсоре.

ПС «АРМ УС» предоставляет администратору безопасности СОВ возможность задавать набор правил для обслуживаемых сенсоров.

ПС «АРМ УС» предоставляет администратору безопасности СОВ возможность задавать приоритеты и флаги критичности атак для каждого конкретного сенсора или группы сенсоров.

ПС «АРМ УС» предоставляет удаленный доступ к технологическим возможностям ПС «Сенсор» и ПС «Сервер УС» посредством сетевого подключения к специальной командной оболочке.

ПС «АРМ УС» использует ролевую модель разграничения доступа, строящуюся на собственных механизмах аутентификации и идентификации пользователя (с вводом наименования учетной записи и пароля администратора безопасности или оператора визуального контроля СОВ) и сверкой введенных данных со значениями, содержащимся в локальной базе пользователей.

В случае обнаружения сетевых вторжений, аномалий сетевого трафика и нарушений безопасности ПС «АРМ УС»:

а) выдает данные об автоматическом блокировании вторжения;

б) выдает запрос на автоматизированное блокирование вторжения;

в) уведомляет администраторов системы безопасности и операторов визуального контроля о возникающих вторжениях визуально и методом отправки сообщений на электронную почту.

ПС «АРМ УС» дает возможность администратору безопасности СОВ настраивать почтовые адреса получателей и правила отсылки сообщений электронной почты о выявленных сетевых вторжениях.

ПС «АРМ УС» дает возможность администратору безопасности СОВ настраивать правила автоматического и автоматизированного назначения правил.

ПС «АРМ УС» дает возможность администратору безопасности СОВ создавать новых администраторов безопасности и операторов визуального контроля СОВ, как учетные записи ОПО ОС, так и внутренней ролевой модели.

ПС «АРМ УС» предоставляет администратору безопасности СОВ возможность конфигурации модели иерархического взаимодействия с целью определения порядка подчиненности.

ПС «АРМ УС» предоставляет администратору безопасности СОВ возможность настройки на ПС «Сервер УС» списка выявленных сетевых вторжений и аномалий для передачи в рамках иерархической модели взаимодействия.

ПС «АРМ УС» реализует возможность просмотра информации о состоянии сенсора (данные о доступности сенсора, запущенных процессах анализа трафика, целостности конфигурационных файлов, проценте использования ресурсов и дате последнего останова) с использованием методов картографирования местности, на которой расположены обслуживаемые сенсора.

ПС «АРМ УС» выполняет индикацию статистической информации об источниках происхождения сетевых атак на карте мира, с цветовой градацией количества и степени серьезности угроз сетевых вторжений.

ПС «АРМ УС» выполняет индикацию оперативной информации о странах – источниках сетевых вторжений, на карте мира, с применением методов цветовой градации уровня угрозы.

ПС «АРМ УС» реализует функции системы управления событиями безопасности (SIEM-система).

ПС «АРМ УС» поддерживает механизмы автоматизированной выборки информации о сетевых вторжениях, содержащейся в базе данных, а также осуществляет её визуализацию. При работе с данным модулем администратор безопасности и оператор визуального контроля имеет возможность:

а) выбирать таблицу базы данных сетевых вторжений, из которой производится выборка информации о сетевых вторжениях;

б) получать статистическую информацию о компьютерных атаках, хранящихся в базе данных;

в) задавать диапазон времени, за который производится выборка;

г) задавать контролируемую систему, идентификатор сенсора, а также отдельные IP-адреса;

д) выбирать направление атак относительно контролируемой системы;

е) просматривать и редактировать описания атак;

ж) выбирать из таблицы информацию о компьютерных атаках по конкретному IP-адресу;

з) выбирать из таблицы информацию о компьютерных атаках по идентификатору атаки;

и) получать данные о стране – источнике сетевого вторжения, посредствам системы GeoIP;

к) выбирать информацию из базы данных по любому полю таблицы с СИБ;

л) выбирать наиболее активно атакующие IP-адреса за исследуемый промежуток времени или наиболее атакуемые объекты; при этом есть возможность выбора отдельных сенсоров и контролируемых систем;

м) выбирать наиболее часто встречающиеся сетевые вторжения: по приоритетам и их количеству, за исследуемый период на конкретный IP-адрес,

на конкретном сенсоре, в конкретной контролируемой подсети, по всем ресурсам в целом.

ПС «Сервер УС» реализует функции контроля целостности своего ПО и конфигурационных файлов:

а) при старте ПО;

б) по установленным временным интервалам;

в) по команде администратора безопасности и оператора визуального контроля СОВ с ПС «АРМ УС».

ПС «АРМ УС» реализует механизмы самотестирования функций журналирования событий, авторизации администратора и оператора безопасности СОВ, контроля целостности и получения СИБ:

а) при старте изделия;

б) по установленным временным интервалам;

в) по команде администратора безопасности и оператора визуального контроля СОВ.

По результатам выполнения функций самотестирования ПС «АРМ УС» оповещает администратора безопасности и оператора визуального контроля СОВ.

ПС «АРМ УС» журналирует события в части:

а) выполнения функций авторизации;

б) запуска и останова ПС «АРМ УС»;

в) чтение данных журналирования событий;

г) выполнения действий по управлению;

д) изменения базы данных сетевых вторжений;

е) изменения базы решающих правил сигнатурного анализа;

ж) изменения базы решающих правил на сенсорах, группах сенсоров;

з) изменения статистических критериев статистического анализатора;

и) автоматического и автоматизированного применение правил;

к) изменения состояния ролей учетных записей администраторов безопасности и операторов визуального контроля СОВ;

л) изменения системного времени;

м) результатов контроля целостности;

н) результатов самотестирования.

ПС «АРМ УС» связывает каждое журналируемое событие безопасности под наименованием учетной записи администратора:

а) с датой и временем возникновения события;

б) с идентификатором процесса;

в) с результатом выполнения.

ПС «АРМ УС» дает администратору безопасности СОВ возможность импорта журналов безопасности с ПС «Сенсор» и ПС «Сервер УС» для проведения аудита безопасности.

ПС «АРМ УС» предоставляет администратору безопасности следующие возможности по управлению журналами безопасности:

а) аудит содержимого журналов безопасности;

б) копирование журналов безопасности на различные носители информации;

в) изготовление твердых копий (печать) журналов безопасности;

г) удаление журналов безопасности.

Любое действие администратора безопасности СОВ с журналами безопасности регистрируется системой журналирования ПС «АРМ УС».

ПС «АРМ УС» позволяет администратору безопасности СОВ выполнять аудит событий безопасности в полученных с ПС «Сенсор» и ПС «Сервер УС» журналах безопасности.

ПС «АРМ УС» выполняет аудит событий в журналах безопасности:

а) по наименованиям записей;

б) по номерам (группам номеров) записей;

в) по результатам выполнения;

г) по диапазону датам и времени возникновения;

д) по адресам и идентификаторам источников событий.

Перечень терминов и сокращений

| | | |
|---|---|---|
| АПК | – | аппаратно-программный комплекс |
| БД | – | база данных |
| ИПБ | – | информационный пакет безопасности |
| КА | – | компьютерная атака |
| НЖМД | – | накопитель на жестких магнитных дисках |
| ОА | – | объект атаки |
| ОКР | – | опытно-конструкторская работа |
| ОПО | – | общее программное обеспечение |
| ОС | – | операционная система |
| ПАК | – | программно-аппаратный комплекс |
| ПО | – | программное обеспечение |
| ПС | – | программное средство |
| ПЭВМ | – | персональная электронная вычислительная машина |
| СА | – | субъект атаки |
| СКЗИ | – | средство криптографической защиты |
| СОВ | – | система обнаружения вторжений |
| ПО | – | программное обеспечение |
| СС | – | состояние сенсоров |
| СУБД | – | система управления базами данных |

Лист регистрации изменений

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

Ф.2.503-3