УТВЕРЖДЕН
ФДШИ.03618-01 31 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ «РЕБУС-СОВ»

Описание применения

ФДШИ.03618-01 31 01

Листов 35

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

2020

Литера $О_1$

АННОТАЦИЯ

В данном документе приведены сведения о назначении, условиях применения, описании задачи, входных и выходных данных изделия ФДШИ.03618-01 «Программный комплекс обнаружения вторжений «Ребус-СОВ» (далее – ПК «Ребус-СОВ»).

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение и область применения

ПК «Ребус-СОВ» предназначен для функционирования на уровне сети и на уровне узлов информационной системы (ИС) с целью обнаружения и блокирования угроз безопасности информации, относящихся к вторжениям (атакам):

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

ПК «Ребус-СОВ» применяется в качестве элемента системы защиты информации информационных систем, функционирующих на базе вычислительных сетей и обрабатывающих государственную тайну и (или) конфиденциальную информацию, включая персональные данные.

1.2. Функциональные возможности

ПК «Ребус-СОВ» обеспечивает выполнение следующих функций:

1) обнаружение вторжений на основе анализа сетевого трафика, проходящего через контролируемый узел ИС (станцию), в режиме, близком к реальному масштабу времени;
2) обнаружение вторжений на основе анализа журналов аудита операционной системы и прикладного ПО;
3) обнаружение вторжений на основе анализа журналов аудита ФДШИ.469535.048 «Модернизированный аппаратно-программный комплекс защиты информации (АПКЗИ «Ребус-М»)»;
4) оперативное отображение информации о вторжениях, обнаруженных на контролируемых станциях;
5) отображение состояния агентских станций;
6) визуализация собранной статистики о вторжениях;
7) централизованное управление блокировкой станций и сетевого трафика;
8) формирование отчетов с возможностью задания правил фильтрации и сохранения отфильтрованной информации в отдельных файлах.

1.3. Основные характеристики

ПК «Ребус-СОВ» позволяет обнаруживать вторжения на ЭВМ, объединенных в вычислительную сеть и функционирующих под управлением ОС семейства Windows, ОС МСВС и ОС СН «Astra Linux Special Edition».

ПК «Ребус-СОВ» реализует методы обнаружения вторжений на уровне сети и уровне узлов информационной системы, а также методы противодействия вторжениям, работающие в ручном и в автоматическом режимах.

В ПК «Ребус-СОВ» входят следующие составные части:

- ФДШИ.03619-01«Консоль управления СОВ»;
- ФДШИ.03620-01«Сервер СОВ»;
- ФДШИ.03621-01 «Агент СОВ»;
- ФДШИ.03622-01«Средство сбора данных и обнаружения вторжений»;
- ФДШИ.03623-01«Средство противодействия вторжениям».

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к составу технических средств

Для функционирования программы должны использоваться ЭВМ со следующими техническими характеристиками:

- ЭВМ типа IBM PC с Intel x86/x64-совместимым процессором не ниже Pentium IV 3 ГГц, либо ЭВМ на базе процессора Эльбрус-8С;
- минимальный объем оперативной памяти – 2 Гбайт, рекомендуемый объем оперативной памяти – не менее 4 Гбайт;
- свободное место на системном разделе жесткого диска – не менее 1 Гбайт;
- поддержка монитором и видеоадаптером ЭВМ рабочих разрешений не менее 1024x768 точек при глубине цвета не менее 8 бит (для рабочего места оператора);
- клавиатура и мышь или совместимое устройство ввода;
- сетевой адаптер (поддерживающий скорость не менее 10 Мбит/с).

ЭВМ должны быть объединены в вычислительную сеть. Сеть должна быть настроена на использование стека сетевых протоколов TCP/IPv4.

2.2. Требования к общесистемному программному обеспечению

В качестве операционной системы (ОС) для ПК «Ребус-СОВ» должны использоваться:

- ОС Microsoft Windows 7 SP1/8/8.1/10/Server 2008 R2 SP1/Server 2016/Server 2019/Server 2022;
- ОС МСВС 5.0 ЦАВМ.11004-01 (изменение № 7);
- ОС СН «Astra Linux Special Edition» РУСБ.10015-01 (релиз «Смоленск» версии 1.4, 1.5, 1.6);
- ОС СН «Astra Linux Special Edition» РУСБ.10265-01 (релиз «Ленинград» версия 8.1).

2.3. Требования к среде эксплуатации

На ЭВМ, предназначенных для эксплуатации изделия, не должно быть установлено других СОВ. В прикладном и общем программном обеспечении должно быть исключено применение средств программирования и отладки.

До начала эксплуатации изделия необходимо убедиться в отсутствии вредоносного ПО на ЭВМ. В случае его обнаружения оно должно быть удалено с ЭВМ. При развертывании ПК «Ребус-СОВ» нежелательно, чтобы ЭВМ эксплуатировалась до полного развертывания на ней ПК «Ребус-СОВ».

Для обеспечения возможности уведомления администраторов СОВ о вторжениях путем отправки сообщений по электронной почте необходимо наличие в сети почтового сервера. Почтовый сервер должен располагаться на ЭВМ со статическим IP-адресом и быть доступным по локальной вычислительной сети (ЛВС) с сервера СОВ по протоколу SMTP. Почтовый сервер должен иметь возможность настройки аутентификации входящих сообщений.

ОС СН «Astra Linux Special Edition» версий 1.4 и 1.5 релиз «Смоленск» должны быть установлены следующие компоненты:

- libqtwebkit4;
- libcrypto++9.

ОС СН «Astra Linux Special Edition» версии 1.6 релиз «Смоленск» должны быть установлены следующие компоненты:

- insserv;
- libqtwebkit4;
- libcrypto++6.

ОС СН «Astra Linux Special Edition» релиз «Ленинград» должны быть установлены следующие компоненты:

- libpcap0.8;
- insserv;
- libqtwebkit4.

Данные пакеты присутствует на дистрибутивном диске ОС, однако по умолчанию могут не установиться. До начала установки ПК «Ребус-СОВ» администратору необходимо с помощью стандартного менеджера пакетов ОС установить эти пакеты.

ПК «Ребус-СОВ» поддерживает режим замкнутой программной среды ОС СН «Astra Linux Special Edition». Подготовка к работе в режиме замкнутой программной среды описана в разделе 3 ФДШИ.03618-01 34 01 «Руководство оператора».

2.4. Рекомендации по составу и квалификации обслуживающего персонала

Эксплуатация изделия возможна только при условии наличия на объекте должностного лица, выполняющего роль администратора СОВ. Данное должностное лицо может совмещать обязанности оператора СОВ, однако рекомендуется разделить обязанности оператора и администратора. Количество должностных лиц, выполняющих роли администратора и оператора, зависит от особенностей объекта информатизации.

Администратором рекомендуется назначать специалиста, знакомого с архитектурой сетей, с принципами функционирования сетей и имеющего опыт администрирования в ОС Windows и ОС СН «Astra Linux Special Edition».

Оператором рекомендуется назначать специалиста, обладающего знаниями в области компьютерных атак.

2.5. Организация мер безопасности

На ЭВМ, предназначенных для эксплуатации изделия, должны функционировать средства защиты уровня ОС, обеспечивающие аутентификацию и идентификацию пользователя, а также разграничение доступа к файловым ресурсам ЭВМ.

После установки ПК «Ребус-СОВ» администратор безопасности должен настроить права доступа на файлы журнала аудита таким образом, чтобы доступ был разрешен только администраторам и операторам ПК «Ребус-СОВ». Для ОС Windows файлы журнала аудита располагаются в каталоге **%ALLUSERSPROFILE%\rebus-sov\log**, для ОС МСВС и ОС СН «Astra Linux Special Edition» – в каталоге **/var/log/rebus-sov**.

В ОС Windows для администраторов и операторов ПК «Ребус-СОВ» необходимо настроить разрешение на запуск и использование ПО ПК «Ребус-СОВ». Пользователям ИС, которые не являются пользователями СОВ, необходимо запретить доступ к ПО ПК «Ребус-СОВ», находящемуся в каталоге **%PROGRAMM FILES%CPS\rebus-sov** в 32-битных конфигурациях ОС Windows или в каталоге **%PROGRAMM FILES (x86)%CPS\rebus-sov** в 64-битных конфигурациях ОС Windows. К конфигурационному файлу **time_sync.conf**, расположенному в каталоге **%ProgramData%\CPS\rebus-sov\ipsCommon**, необходимо разрешить доступ только администраторам СОВ. В ОС МСВС и ОС СН «Astra Linux Special Edition» дополнительные настройки не требуются.

На объекте эксплуатации должна быть разработана и применена политика назначения и смены паролей пользователей СОВ. Политика назначения и смены паролей должна предусматривать использование безопасных паролей в соответствии с требованиями к паролям для класса ИС, в которой развернута СОВ. Должна быть предусмотрена процедура периодической смены паролей, а также процедура немедленной смены паролей в случае дискредитации аутентификационных данных пользователей и администраторов СОВ.

2.6. Идентификация режимов работы ПК «Ребус-СОВ»

При эксплуатации ПК «Ребус-СОВ» возможны следующие режимы работы изделия:

- нормальный режим. Нормальный режим характеризуется отсутствием каких-либо инцидентов в защищаемой ИС и отсутствием вторжений. Консоль управления в данном случае не

отображает информации о вторжениях, в отношении которых не было принято мер;

- обнаружено вторжение. Данный режим идентифицируется наличием сообщений о вторжениях в консоли управления. Панель «Текущее состояние» отображается красным цветом. Оператор должен проанализировать информацию о вторжении и в случае необходимости выполнить блокировку станции/сетевого трафика станции, с которой пришло данное сообщение. Дополнительно может быть проведено антивирусное сканирование объектов файловой системы на данной ЭВМ;

- выполнена блокировка агентской станции. Блокировка может быть выполнена автоматически либо по запросу из консоли управления. Действующие для станции блокировки отображаются во вкладке «Станции» консоли управления. Необходимо устранить причины блокировки и выполнить ее снятие;

- на агентской станции произошел сбой в работе компонентов ПК «Ребус-СОВ». ПК «Ребус-СОВ» осуществляет попытку автоматического перезапуска компонентов в случае обнаружения сбоя. При этом регистрируются событие, содержащее информацию о модуле, в работе которого возникли проблемы, и результат перезапуска. В случае невозможности перезапуска компонента либо периодического повторения проблемы необходимо выявить и устранить ее причины. Для этого необходимо проанализировать события, регистрируемые ПК «Ребус-СОВ» на данной станции, а также журналы ОС. В случае если проблемы начались после обновления сигнатур вторжений, необходимо вернуть предыдущую версию.

2.7. Схема размещения ПК «Ребус-СОВ» в ИС

ПК «Ребус-СОВ» может обеспечивать обнаружение вторжений на уровне сети и на уровне узла. В случае работы на уровне сети ПК «Ребус-СОВ» устанавливается на шлюз либо на ЭВМ, подключенную к сетевому ответвителю или SPAN-порту коммутатора. В случае работы на уровне узла ПК «Ребус-СОВ» должен быть установлен на каждый защищаемый узел сети. В обоих случаях на ЭВМ должна быть установлена агентская часть ПК «Ребус-СОВ». Сервер СОВ рекомендуется расположить на выделенной ЭВМ. Сервер СОВ должен быть доступен по сети со всех агентских станций. При установке ПК «Ребус-СОВ» необходимо выбрать «Сервер СОВ».

2.8. Условия совместной работы с антивирусным ПО

ПК «Ребус-СОВ» в своих базах сигнатур может содержать сигнатуры вирусного ПО. Это может вызвать ложные срабатывания антивирусного ПО. Конкретно это зависит от состава вирусных баз самого антивирусного ПО.

Если такие ложные срабатывания возникают, то необходимо в исключения антивируса добавить каталоги **/usr/local/CPS/rebus-sov** в ОС СН «Astra Linux Special Edition» и ОС МСВС и **C:\ProgramData\CPS\rebus-sov** в ОС Windows.

Также возможны ложные срабатывания при получении пакета обновлений сигнатур. Если такое происходит, то можно на время получения и установки пакета обновлений отключать антивирусный мониторинг.

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Общие положения

ПК «Ребус-СОВ» позволяет решать следующие задачи:
- обнаружение вторжений в информационной системе;
- регистрация обнаруженных вторжений;
- анализ обнаруженных вторжений;
- реагирование на обнаруженные вторжения;
- контроль состояния СОВ;
- учет специфики контролируемой информационной системы;
- управление доступом к данным и функциям СОВ.

3.2. Роли пользователей СОВ

Для решения перечисленных выше задач в ПК «Ребус-СОВ» предусмотрены две предустановленные роли пользователей – администратор и оператор. Администратор СОВ должен являться администратором в ОС. В качестве оператора СОВ может выступать обычный непривилегированный пользователь ОС.

Задачи оператора СОВ:
- обнаружение вторжений;
- анализ обнаруженных вторжений;
- реагирование на обнаруженные вторжения;
- контроль состояния СОВ.

Задачи администратора СОВ:
- установка и деинсталляция ПК «Ребус-СОВ»;
- настройка ПК «Ребус-СОВ»;
- проведение мероприятий по устранению последствий вторжений: локальное снятие выполненных блокировок, запуск антивирусного сканирования, переустановка ОС;
- восстановление работоспособности ПК «Ребус-СОВ» в случае обнаружения проблем функционирования;
- обновление сигнатур вторжений СОВ;
- управление доступом к данным и функциям СОВ.

Кроме того, администратору СОВ доступны все возможности оператора СОВ.

Далее по тексту для обозначения случаев, относящихся и к администраторам, и к операторам СОВ, используется термин «пользователи СОВ».

3.3. Обнаружение вторжений в информационной системе

Обнаружение вторжений в контролируемой ИС необходимо для регистрации сведений о выполняемых вторжениях (с целью последующего анализа и аудита), а также для обеспечения возможности оперативного реагирования на эти вторжения.

Применение ПК «Ребус-СОВ» позволяет использовать в ИС следующие способы обнаружения вторжений:
- анализ сетевого трафика, проходящего через контролируемые узлы ИС;
- анализ журналов аудита операционной системы и прикладного ПО;
- анализ журналов аудита ФДШИ.469535.048 «Модернизированный аппаратно-программный комплекс защиты информации (АПКЗИ «Ребус-М»)»;
- анализ статистики сетевого трафика.

Анализ сетевого трафика осуществляется в режиме, близком к реальному масштабу времени, и включает в себя сигнатурный анализ и анализ состава ЛВС.

Сигнатурный анализ сетевого трафика обеспечивает выявление вторжений путем сопоставления информации из сетевых пакетов и сигнатур вторжений формата SNORT.

Анализ состава ЛВС обеспечивает выявление активных (генерирующих сетевой трафик) сетевых устройств (ЭВМ, сетевых периферийных устройств, коммуникационного оборудования), нештатно подключенных к защищаемому сегменту сети. Выявление осуществляется путем сопоставления данных из заголовков сетевых пакетов (IP-, MAC-адреса) и соответствующих сведений из списка доверенных сетевых устройств.

Анализ журналов аудита ОС и ПО использует для выявления вторжений журналы событий и лог-файлы ОС (Windows, МСВС, Astra Linux Special Edition), а также различное прикладное ПО. События из указанных источников считываются в оперативном режиме и анализируются с использованием сигнатур вторжений формата OSSEC.

Анализ журналов аудита АПКЗИ «Ребус-М» использует в качестве источника данных журнал регистрации событий ФДШИ.01792-06 «Модернизированный аппаратно-программный комплекс защиты информации (АПКЗИ «Ребус-М»). Программное обеспечение для ОС семейства Windows», фиксируя в качестве вторжений заданные события попыток несанкционированного доступа.

ПК «Ребус-СОВ» позволяет дополнять описанные выше способы обнаружения вторжений новыми путем установки дополнительных программных компонентов, автоматически интегрируемых в комплекс.

Анализ статистики сетевого трафика обеспечивает выявление вторжений методом подсчета количества сетевых потоков за определенный интервал времени. Если количество потоков превышает допустимое, то регистрируется вторжение.

Обнаружение вторжений осуществляется на всех станциях с установленным ПК «Ребус-СОВ» в автоматическом режиме в соответствии с заданными настройками.

В случае изменения политики безопасности или штатного состава ЛВС на объекте эксплуатации необходимо выполнить настройку ПК «Ребус-СОВ» для соответствия новым реалиям. Настройка осуществляется администратором с помощью консоли управления СОВ.

Для обеспечения возможности выявления новых видов вторжений необходимо своевременно осуществлять обновление сигнатур вторжений. Пакеты обновлений сигнатур вторжений предоставляются разработчиком ПК «Ребус-СОВ». Процесс обновления выполняется администратором с помощью консоли управления СОВ.

3.4. Регистрация обнаруженных вторжений

Сведения об обнаруженных вторжениях должны регистрироваться. Это необходимо для обеспечения возможности последующего анализа обстановки и аудита.

При использовании ПК «Ребус-СОВ» сведения об обнаруженных вторжениях автоматически передаются по сети на станцию – сервер СОВ и регистрируются на ней в архивах событий аудита. В случае отсутствия связи с сервером СОВ собранные сведения сохраняются локально на станции, выявившей вторжение, и передаются на сервер СОВ при появлении связи с ним.

При регистрации фиксируются следующие сведения о вторжениях:

- дата и время обнаружения вторжения;
- станция, на которой обнаружено вторжение;
- источник сведений о вторжении (например, «Анализатор сетевого трафика», «Анализатор состава ЛВС», «Анализатор событий ОС и ПО» и т.п.);
- тип события (например, «Обнаружено нештатное сетевое устройство», «Попытка несанкционированного обращения к USB-порту», «Ошибка авторизации» и т.п.);
- реакция на событие (при ее осуществлении);
- специфичная информация о вторжении (зависит от источника и типа события).

Для предотвращения переполнения диска сервера СОВ событиями аудита, а также для обеспечения удобства резервного копирования архивов событий аудита в ПК «Ребус-СОВ» реализована возможность архивирования журнала аудита при его переполнении и по истечении определенного промежутка времени. Консоль управления позволяет задать максимальное количество событий в журнале аудита, а также временной интервал (ежедневно, еженедельно,

ежемесячно, ежегодно, никогда), по истечении которого произойдет автоматическое архивирование журнала аудита. В результате архивирования формируется отдельный файл-архив, который располагается в том же каталоге, что и текущий журнал аудита **%ALLUSERSPROFILE%\rebus-sov** для ОС семейства Windows и **/var/log/rebus-sov** для ОС МСВС и ОС СН «Astra Linux Special Edition». В дальнейшем файл-архив может быть перемещен на внешний носитель информации либо (при отсутствии надобности в нем, например, по истечении срока давности) удален. По завершении процесса архивирования текущий журнал аудита не содержит записей. Факт архивирования журнала аудита регистрируется в журнале аудита.

В случае нехватки места на диске и невозможности записи вновь поступающих событий ПК «Ребус-СОВ» удаляет самый старый файл-архив, фиксируя данный факт в журнале аудита. Для предотвращения подобных ситуаций ПК «Ребус-СОВ» осуществляет периодический автоматический контроль наличия свободного места в разделе с журналом аудита. В случае если объем доступного свободного места оказывается меньше заданного порогового значения, осуществляется регистрация соответствующего служебного события.

Формируемые архивы событий аудита могут в дальнейшем использоваться для формирования отчетов по вторжениям.

3.5. Анализ обнаруженных вторжений

Сведения об обнаруженных вторжениях должны анализироваться для оценки обстановки по вторжениям, обеспечения возможности оперативного реагирования на вторжения, выяснения обстоятельств конкретных вторжений с целью оценки их масштаба и последствий, выявления существующих в ИС каналов осуществления вторжений, предпосылок и причин возможности реализации вторжений с целью последующей организации мер по предотвращению подобных вторжений в дальнейшем и т.п.

Анализ обнаруженных вторжений с помощью ПК «Ребус-СОВ» может осуществляться в оперативном режиме и по мере необходимости (по запросу).

Оперативный анализ вторжений может осуществляться как автоматически, так и вручную пользователем СОВ.

Автоматический оперативный анализ вторжения осуществляется ПК «Ребус-СОВ» на станции, обнаружившей вторжение, путем сопоставления сведений о нем (источник, тип вторжения) с заданными настройками автоматического реагирования.

Ручной оперативный анализ вторжений осуществляется пользователем СОВ путем просмотра информации о вторжениях, оперативно и централизованно отображаемой в консоли управления СОВ. Состав отображаемых в консоли управления СОВ сведений о вторжениях соответствует составу регистрируемых сведений и приведен в 3.4.

Также оперативный анализ вторжений (но с меньшей степенью оперативности) возможен путем просмотра сообщений электронной почты, рассылаемых ПК «Ребус-СОВ» администраторам СОВ и содержащих статистические сведения (по источникам и типам) о вторжениях, произошедших в ИС за заданный период времени.

Помимо сведений об отдельных вторжениях, в консоли управления СОВ отображаются статистические данные по обнаруженным вторжениям, которые также могут использоваться пользователями СОВ для анализа текущей обстановки по вторжениям в ИС.

Анализ вторжений по запросу осуществляется пользователем СОВ с помощью генерируемых ПК «Ребус-СОВ» отчетов по обнаруженным вторжениям. Отчеты генерируются по запросу пользователя из консоли управления СОВ на основании данных одного или нескольких архивов журнала аудита, при этом возможно задавать фильтры по времени регистрации, по станции, обнаружившей вторжение, по источнику событий и т.п. Отчеты формируются в виде файлов формата HTML (в ОС Windows дополнительно PDF) и могут просматриваться любыми средствами просмотра, поддерживающими эти форматы (при запуске просмотра из консоли управления СОВ используется текущее зарегистрированное в ОС средство просмотра).

3.6. Реагирование на обнаруженные вторжения

Для прерывания продолжительных по времени вторжений (например, DOS-атак, сканирования сетевых портов, попыток подбора пароля и т.п.), а также для предотвращения последующих аналогичных вторжений необходимо своевременное реагирование на обнаруженные вторжения. Данная задача при использовании ПК «Ребус-СОВ» может решаться в ИС автоматически, автоматизированно и вручную.

Для автоматического и автоматизированного реагирования на вторжения ПК «Ребус-СОВ» предоставляет возможность блокирования сетевого трафика.

Блокировка станции доступна для станций, на которых установлено ПО АПКЗИ «Ребус-М» для ОС семейства Windows (ФДШИ.01792-06). ПК «Ребус-СОВ» передает в АПКЗИ «Ребус-М» команду заблокировать станцию для пользователя, в результате чего работа пользователя на станции будет невозможна; в том числе будут блокироваться все файловые операции приложений, работающих от имени пользователя.

ВНИМАНИЕ! Данный вид блокировки не сработает, если на станции зарегистрирован администратор АПКЗИ!

Блокировка сетевого трафика осуществляется средствами ПК «Ребус-СОВ». Данная блокировка может использоваться как для блокировки трафика, приходящего на станцию с заданного IP-адреса, так и для полной блокировки сетевого трафика ЭВМ (за исключением служебного трафика ПК «Ребус-СОВ»).

ПК «Ребус-СОВ» позволяет дополнять описанные выше реакции новыми путем установки дополнительных программных компонентов, автоматически интегрируемых в комплекс.

Автоматическое реагирование на вторжения выполняется ПК «Ребус-СОВ» на станции, обнаружившей вторжение, в соответствии с настроенными в ПК «Ребус-СОВ» правилами. Настройка правил автоматического реагирования осуществляется централизованно в консоли управления СОВ путем сопоставления требуемых параметров вторжения (источник, тип вторжения) и необходимой реакции.

Автоматизированное реагирование (по запросу) на вторжения выполняется пользователем СОВ централизованно путем управления реакциями на станциях из консоли управления СОВ. Пользователь осуществляет блокировку, руководствуясь сведениями о вторжениях, отображаемыми в консоли управления, а также информацией, полученной по другим каналам.

Снятие установленных (как автоматически, так и автоматизированно) блокировок может осуществляться как централизованно из консоли управления СОВ, так и локально с помощью средства настройки агентской части.

Ручное реагирование выполняется пользователем СОВ на основании сведений, полученных от ПК «Ребус-СОВ» либо из других источников. Данный способ реагирования осуществляется без прямого участия ПК «Ребус-СОВ» с помощью организационных, технических и организационно-технических средств, доступных пользователю на объекте информатизации (например, перенастройка межсетевого экрана, логическое или физическое отключение ЛВС от Интернета, отправка группы реагирования к контролируемой станции и т.п.).

Оператор СОВ должен проанализировать информацию о вторжении и в случае необходимости проведения работ по устранению последствий вторжения известить администратора СОВ.

3.7. Контроль состояния СОВ

Для контроля текущей защищенности ИС от вторжений необходимо постоянно осуществлять контроль состояния СОВ. ПК «Ребус-СОВ» обеспечивает два направления решения этой задачи:

- контроль состояния компонентов СОВ;
- аудит служебных событий СОВ.

Данная задача выполняется оператором СОВ. В случае обнаружения проблем в работе СОВ оператор СОВ должен незамедлительно уведомить администратора СОВ.

Контроль состояния компонентов СОВ осуществляется с помощью консоли управления СОВ путем просмотра отображаемых в ней сводных статистических данных по активности агентов СОВ, а также путем просмотра текущего состояния станции (подключена к серверу СОВ, не прошла аутентификацию на сервере СОВ, недоступна по сети и т.п.), наличия, состояния (запущен, остановлен) и версий отдельных механизмов СОВ (плагинов), а также действующих на станции блокировок.

Аудит служебных событий СОВ осуществляется путем просмотра зарегистрированных служебных событий в оперативном режиме в консоли управления либо в отчете по событиям аудита, содержащем служебные события СОВ. Состав сведений, регистрируемых для служебных событий, соответствует составу регистрируемых сведений о вторжении, приведенному в 3.4, за исключением реакции.

Сведения о служебных событиях, регистрируемых ПК «Ребус-СОВ», приведены в таблице 1.

Таблица 1 – События, регистрируемые ПК «Ребус-СОВ»

Источник события	Тип события	Дополнительная информация	Результат
Агент СОВ	Запуск агента СОВ	Не предусмотрена	Успешно
Агент СОВ	Остановка агента СОВ	Не предусмотрена	Успешно
Агент СОВ	Плагин успешно запущен	Имя плагина	Успешно
Агент СОВ	Ошибка запуска плагина	Имя плагина. Подробности ошибки	Неуспешно
Агент СОВ	Плагин успешно остановлен	Имя плагина	Успешно
Агент СОВ	Ошибка остановки плагина	Имя плагина. Подробности ошибки	Неуспешно
Агент СОВ	Запуск плагина	Имя плагина	Успешно
Агент СОВ	Перезапуск плагина	Имя плагина	Успешно
Агент СОВ	Ошибка перезапуска плагина	Имя плагина. Подробности ошибки	Неуспешно
Агент СОВ	Ошибка подключения плагина	Имя плагина. Подробности ошибки	Успешно
Агент СОВ	Настройки перечитаны	Не предусмотрена	Успешно
Агент СОВ	Выполнено локальное снятие блокировки	Не предусмотрена	Успешно
Агент СОВ	Обнаружен новый плагин	Имя плагина	Успешно
Агент СОВ	Синхронизация времени средствами агента отключена в файле настроек	Не предусмотрена	Успешно
Агент СОВ	Время синхронизировано с сервером	Текущее время	Успешно
Агент СОВ	Ошибка синхронизации времени с сервером СОВ	Код ошибки	Неуспешно
Агент СОВ	Отсутствует метафайл	Не предусмотрена	Неуспешно
Агент СОВ	Успешно пройдена проверка целостности сигнатур	Не предусмотрена	Успешно
Агент СОВ	Обнаружено нарушение целостности сигнатур	Не предусмотрена	Неуспешно
Агент СОВ	Сигнатуры восстановлены из локального хранилища	Не предусмотрена	Успешно

Продолжение таблицы 1

Источник события	Тип события	Дополнительная информация	Результат
Агент СОВ	Начало обновления сигнатур	Не предусмотрена	Успешно
Агент СОВ	Процесс обновления сигнатур завершен	Не предусмотрена	Успешно
Агент СОВ	Обновление сигнатур не требуется	Не предусмотрена	Успешно
Агент СОВ	Сигнатуры восстановлены из хранилища сервера	Не предусмотрена	Успешно
Агент СОВ	Ошибка обновления сигнатур из хранилища сервера	Код ошибки	Неуспешно
Агент СОВ	Самотестирование плагина агента СОВ	Имя плагина	Успешно
		Имя плагина. Описание ошибки	Неуспешно
Агентский плагин «Анализатор событий ОС и ПО»	Задача перезапущена	Не предусмотрена	Успешно
Агентский плагин «Анализатор событий ОС и ПО»	Задача не может быть перезапущена	Не предусмотрена	Неуспешно
Агентский плагин «Анализатор событий ОС и ПО»	Аварийное завершение задачи	Наименование задачи	Неуспешно
Агентский плагин «Плагин блокировки сетевого трафика»	Выполнена блокировка IP-адреса	Параметры блокировки	Успешно
Агентский плагин «Плагин блокировки сетевого трафика»	Выполнена разблокировка IP-адреса	Параметры разблокировки	Успешно
Агентский плагин «Плагин блокировки сетевого трафика»	Не удалось выполнить блокировку IP-адреса	Параметры блокировки	Неуспешно
Агентский плагин «Плагин блокировки сетевого трафика»	Не удалось выполнить разблокировку IP-адреса	Параметры разблокировки	Неуспешно
Агентский плагин «Плагин блокировки сетевого трафика»	Выполнена разблокировка всех IP-адресов	Не предусмотрена	Успешно
Агентский плагин «Плагин блокировки сетевого трафика»	Не удалось выполнить разблокировку всех IP-адресов	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Невозможно запустить Snort	Не предусмотрена	Неуспешно

Продолжение таблицы 1

Источник события	Тип события	Дополнительная информация	Результат
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Невозможно завершить работу компонента анализа сетевого трафика	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Компонент анализа сетевого трафика завершился с кодом <числовой код>	Код завершения	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Процесс Snort не отвечает. Сбор данных невозможен	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Неверный формат внутренних данных	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Неверный формат данных, полученных от Snort	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Ошибка выделения памяти	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Ошибка управления процессом Snort	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Одна из функций ipc_lib вернула ошибку	Не предусмотрена	Неуспешно
Агентский плагин «Средство анализа сетевого трафика с использованием сигнатур»	Попытка запуска процесса Snort, когда он уже запущен	Не предусмотрена	Неуспешно
Средство настройки агента СОВ	Запуск программы настройки агентской части	Не предусмотрена	Успешно
Средство настройки агента СОВ	Установка значения по умолчанию	Не предусмотрена	Успешно

Продолжение таблицы 1

Источник события	Тип события	Дополнительная информация	Результат
Средство настройки агента СОВ	Изменение настроек сетевого взаимодействия СОВ	Старый IP-адрес. Новый IP-адрес	Успешно
Средство настройки агента СОВ	Запуск агента СОВ	Не предусмотрена	Успешно
Средство настройки агента СОВ	Остановка агента СОВ	Не предусмотрена	Успешно
Средство настройки агента СОВ	Локальное снятие блокировок станции	Не предусмотрена	Успешно
Средство настройки агента СОВ	Экспорт ключа аутентификации	Расположение ключа аутентификации	Успешно
		Описание ошибки	Неуспешно
Средство настройки агента СОВ	Закрытие программы настройки агентской части	Не предусмотрена	Успешно
Средство настройки агента СОВ	Верификация целостности модулей	Не предусмотрена	Успешно
Средство настройки агента СОВ	Верификация целостности модулей	Список модулей, не прошедших верификацию	Неуспешно
Средство настройки агента СОВ	Верификация целостности сигнатур	Контрольная сумма сигнатур	Успешно
		Описание ошибки	Неуспешно
Сервер СОВ	Успешное подключение агента	IP-адрес станции	Успешно
Сервер СОВ	Синхронизация времени	Описание событий синхронизации времени	Успешно
		Описание ошибки	Неуспешно
Сервер СОВ	Несоответствие времени на станциях	IP-адрес станции, разница во времени	Неуспешно
Сервер СОВ	Успешное подключение консоли	IP-адрес станции	Неуспешно
Сервер СОВ	Неудачная попытка подключения консоли	IP-адрес станции	Неуспешно
Сервер СОВ	Неудачная попытка подключения агента	IP-адрес станции	Неуспешно
Сервер СОВ	Заканчивается свободное место для хранения событий аудита	Каталог хранения архивов, свободное место на диске	Успешно
Сервер СОВ	Ошибка чтения файла архива	Имя файла, описание ошибки	Неуспешно
Сервер СОВ	Успешно пройдена проверка целостности сигнатур	Не предусмотрена	Успешно
Сервер СОВ	Обнаружено нарушение целостности сигнатур	Не предусмотрена	Неуспешно

Окончание таблицы 1

Источник события	Тип события	Дополнительная информация	Результат
Сервер СОВ	Обнаружено нарушение целостности сигнатур	Каталог сигнатур	Неуспешно
Сервер СОВ	Вывод событий для SIEM включен	Не предусмотрена	Успешно
Сервер СОВ	Вывод событий для SIEM выключен	Не предусмотрена	Успешно
Сервер СОВ	Проверка синхронизации времени отключена	Не предусмотрена	Успешно
Сервер СОВ	Редактирование списка пользователей СОВ	Сетевой адрес станции, с которой происходило редактирование	Успешно
Сервер СОВ	Настройка параметров сервера СОВ	Сетевой адрес станции, с которой происходило редактирование	Успешно
Сервер СОВ	Обновление БРП	Сетевой адрес станции, с которой происходило редактирование	Успешно
Сервер СОВ	Автоматическое обновление БРП	Описание событий автоматического обновления баз	Успешно
Сервер СОВ	Ошибка автоматического обновления БРП	Описание ошибки	Неуспешно
Сервер СОВ	Выполнение сценария управления внешними средствами со станции сервера СОВ	Описание выполнения сценария	Успешно
		Описание ошибки	Неуспешно
Агентский плагин «Анализ статистики сетевого трафика»	Превышено допустимое количество потоков	Количество потоков	Успешно
Агентский плагин «Анализ состава ЛВС»	Обнаружено нештатное сетевое устройство	Сетевые адреса атакующего и атакуемого, кол-во пакетов и направление	Успешно
Агентские плагины «Анализ статистики сетевого трафика» и «Анализ состава ЛВС»	Информация от плагина	Описание выполнения команд сервисом агентского плагина (запуск, остановка, изменение настроек)	Успешно
Агентские плагины «Анализ статистики сетевого трафика» и «Анализ состава ЛВС»	Ошибка работы плагина	Описание ошибки	Неуспешно

3.8. Учет специфики контролируемой информационной системы

При настройке СОВ необходимо учитывать специфику информационной системы, в которой она функционирует.

Учет специфики информационной системы заключается в обеспечении настройки работы механизмов обнаружения и блокирования вторжений на каждой агентской станции. Используя консоль управления СОВ, администратор может отключить или подключить механизмы на выбранной станции. Для каждой агентской станции настройки делаются индивидуально. Например, администратор может отключить механизм анализа сетевого трафика на агентских станциях защищаемого сегмента сети, оставив его только на шлюзе, обеспечив таким образом анализ сетевого трафика уровня сети.

3.9. Управление доступом к данным и функциям СОВ

Для предотвращения вмешательства в штатную работу СОВ доступ к данным и функциям СОВ должен контролироваться.

Данная задача решается как средствами ПК «Ребус-СОВ», так и сторонними средствами защиты уровня ОС.

ПК «Ребус-СОВ» обеспечивает управление доступом к данным и функциям СОВ с помощью учетных записей пользователей СОВ. Для использования консоли управления СОВ пользователь проходит идентификацию и аутентификацию. Далее пользователю разрешается доступ к функционалу, соответствующему его роли (описание ролей пользователей и их задач приведено в 3.2). В частности, управление учетными записями пользователей СОВ, а также их ролями доступно только администратору СОВ.

Доступ к средству настройки агентской части СОВ разрешен только администраторам ОС.

Доступ к данным СОВ на уровне файлов должен управляться средствами защиты информации уровня ОС. Требования по ограничению доступа к данным СОВ описаны в 2.5.

3.10. Маскирование датчиков СОВ

Сетевой датчик ПК «Ребус-СОВ» использует сетевой интерфейс операционной системы и не генерирует сетевой трафик, что делает невозможным выявление датчика стандартными средствами.

Датчики уровня узла представляют собой системные сервисы. Невозможность выявления датчика системы обнаружения вторжений пользователем элемента информационной системы обеспечивается средой функционирования при условии выполнения требований безопасности к среде функционирования, приведенных в 4.9 данного документа.

3.11. Режимы работы анализатора сетевого трафика с использованием сигнатур

Компонент «Анализ сетевого трафика с использованием сигнатур» может работать в двух режимах: пассивном и в разрыве канала.

В пассивном режиме анализатор прослушивает весь входящий трафик ЭВМ и выдает предупреждение в случае обнаружения вторжения, никак не препятствуя самому вторжению.

В режиме разрыва канала анализатор может работать на шлюзе, установленном между двумя сегментами сети. В этом режиме анализатор может блокировать сетевые пакеты, проходящие через шлюз и тем самым предотвращать вторжения.

Режим разрыва канала доступен в ОС СН «Astra Linux Special Edition» релиз «Смоленск» и ОС МСВС. Режим недоступен в ОС СН «Astra Linux Special Edition» релиз «Ленинград» и ОС Windows.

Для использования режима разрыва сети ОС, где анализатор запускается в режиме разрыва канала, должна быть настроена в соответствии с приложением 2 данного документа.

3.12. Сохранение сетевого трафика

Компонент «Анализ сетевого трафика с использованием сигнатур» может сохранять дампы перехваченных сетевых пакетов для их последующего анализа. Возможно сохранение как пакета, неродственно вызвавшего срабатывание правил, так и некоторое количество предшествовавших и последующих пакетов. Возможность сохранения предшествовавших и последующих пакетов доступна только в ОС МСВС 5.0 и ОС СН «Astra Linux Special Edition», релиз «Смоленск». Данные ОС должны использоваться как на агентских станциях, так и на сервере СОВ. Дампы пакетов сохраняются в файл формата pcap.

В один файл сохраняется некоторое количество (настраивается администратором) пакетов до пакета, вызвавшего срабатывание правил, и такое же количество пакетов после. Если после первого пакета, вызвавшего срабатывание правил, был обнаружен ещё один пакет, также вызвавший вторжение, то они все будут сохранены в один файл.

Покажем это на примере. Допустим, администратор настроил компонент «Анализ сетевого трафика с использованием сигнатур» так, что должно сохраняться пять пакетов до и после пакета, вызвавшего срабатывание правил. Все пакеты, попадающие на сетевой интерфейс станции, последовательно попадают в анализатор. Таким образом получается некая последовательность пакетов (рис. 1). Если шестой пакет в этой последовательности вызовет срабатывание какого-либо правила, в файл будут сохранены дампы одиннадцати пакетов: пяти пакетов, предшествующих шестому, самого шестого, и пяти последующих пакетов.

Сохранение пакетов при однократной атаке

Рис. 1

Если после шестого пакета срабатывание правил вызовет, например, восьмого по порядку пакет (рис. 2), то между двумя пакетами, вызвавшими срабатывание правил, интервал будет менее пяти пакетов. В этом случае в файл будет сохранено уже 13 пакетов: пять до первого пакета, вызвавшего срабатывание, пять после последнего пакета, вызвавшего срабатывание и все пакеты между.

Сохранение пакетов при последовательности атак

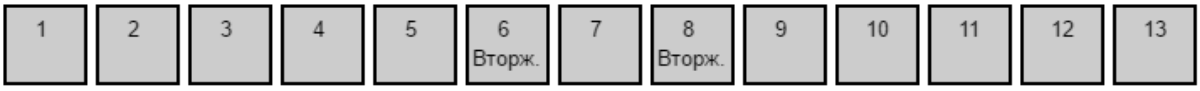

Рис. 2

Настройка сохранения дампов пакетов описана в ФДШИ.03618-01 34 01 «Руководство оператора», раздел 4.

4. РУКОВОДСТВО АДМИНИСТРАТОРА СОВ

4.1. Функции администрирования

Администратор безопасности должен выполнять все функции по развертыванию, настройке, обновлению баз решающих правил и контролю за работой ПК «Ребус-СОВ».

Установка ПК «Ребус-СОВ» выполняется администратором на сервере ПК «Ребус-СОВ», АРМ администратора, рабочих ЭВМ пользователей, серверах сети, служебных ЭВМ с датчиками СОВ, ЭВМ с программными шлюзами и маршрутизаторами. До выполнения установки ПК «Ребус-СОВ» администратор должен выполнить подсчет контрольных сумм модулей дистрибутива и сверить полученные контрольные суммы с эталонными значениями. В процессе установки администратор должен установить в СОВ все необходимые плагины, установить актуальные базы сигнатур вторжений, выполнить конфигурирование СОВ в соответствии со структурой сети передачи данных.

Администратор должен осуществлять контроль за наличием привилегий на администрирование у других пользователей ОС объекта информатизации. Настройка параметров ПК «Ребус-СОВ», касающаяся настройки работы компонентов, также должна осуществляться администратором безопасности. Пользователь может выполнять настройку компонентов ПК «Ребус-СОВ», связанную только с отображением данных.

Изделие ПК «Ребус-СОВ» не требует специального технического обслуживания. Для поддержания изделия в работоспособном состоянии необходимо регулярно выполнять обновление сигнатур вторжений. Установку обновлений сигнатур вторжений должен выполнять администратор. До выполнения обновления сигнатур вторжений администратор обязан выполнить расчет контрольных сумм файлов обновления и сверить полученные контрольные суммы с эталонными значениями, приведенными на сайте разработчика.

4.2. Приемка изделия

Перед установкой ПК «Ребус-СОВ» необходимо убедиться в целостности дистрибутивного носителя. Проверка целостности поставляемого изделия описана в разделе 1 ФДШИ.03618-01 30 01 «Формуляр».

4.3. Интерфейсы, доступные администратору

Администратору доступны интерфейсы модулей, входящих в комплекс ПК «Ребус-СОВ», в том числе:

- модуль установки и удаления ПК «Ребус-СОВ»;
- средство настройки агентской части ПК «Ребус-СОВ»;
- консоль управления ПК «Ребус-СОВ».

Описание интерфейса средства установки приводится в разделе 3 ФДШИ.03618-01 34 01 «Руководство оператора».

Описание интерфейса средства удаления приводится в разделе 3 ФДШИ.03618-01 34 01 «Руководство оператора».

Описание интерфейса средства настройки агентской части приводится в разделе 4 ФДШИ.03618-01 34 01 «Руководство оператора».

Описание интерфейса консоли управления приводится в разделе 4 ФДШИ.03618-01 34 01 «Руководство оператора».

Администратор имеет возможность расширения функционала ПК «Ребус-СОВ» за счет дополнительных компонентов (плагинов). Для добавления новых плагинов необходимо пользоваться средствами ОС, в которой функционирует ПК «Ребус-СОВ». Описание работы с дополнительными плагинами приводится в разделе 4 ФДШИ.03618-01 34 01 «Руководство оператора».

4.4. Управление ПК «Ребус-СОВ»

При помощи интерфейсов программы установки администратор может устанавливать и удалять ПК «Ребус-СОВ», выбирать конфигурации установки. Описание установки приведено в разделе 3 ФДШИ.03618-01 34 01 «Руководство оператора».

Описание удаления ПК «Ребус-СОВ» приведено в разделе 3 ФДШИ.03618-01 34 01 «Руководство оператора».

При помощи консоли управления администратор может настраивать реакции на события СОВ, управлять настройками баз решающих правил.

Для безопасного управления изделием администратор должен пользоваться изделием в соответствии с эксплуатационной документацией. Администратор должен:

- выполнять установку и настройку ПК «Ребус-СОВ»;
- применять средства защиты уровня ОС для обеспечения безопасности данных ПК «Ребус-СОВ», в том числе задавать и периодически менять пароли пользователей на доступ к ПК «Ребус-СОВ»;
- поддерживать в актуальном состоянии набор компонентов ПК «Ребус-СОВ» и баз сигнатур;
- проводить периодический анализ журналов с целью выявления нарушений в работе ПК «Ребус-СОВ»;
- следить за работоспособностью ПК «Ребус-СОВ» и при необходимости выполнять проверку работоспособности отдельных компонентов;
- устранять последствия вторжений (выполнять перенастройку системы, восстанавливать ПО и данные).

Для минимизации потерь информации в случае выхода из строя сервера СОВ администратор должен выполнять периодическое архивирование журнала событий ПК «Ребус-СОВ» и их сохранение на резервном носителе информации. Также администратор СОВ должен выполнять сохранение архивов настроек на резервном носителе информации. При возникновении сбоев в работе ПК «Ребус-СОВ» администратор должен выполнить переустановку ПО, восстановление настроек и сигнатур вторжений.

Дистрибутив ПК «Ребус-СОВ» и сигнатур вторжений должен храниться на резервном носителе информации.

4.5. Контролируемые функции и привилегии

Администратор должен контролировать работу пользователей и не допускать применения пользователями на рабочих местах нештатного программного обеспечения.

Непривилегированные пользователи ОС не должны выполнять перенастройку ЭВМ, перенастройку ЛВС и средств защиты во избежание регистрации ложных событий в СОВ и блокировок.

4.6. Управление пользователями

После установки ПК «Ребус-СОВ» администратор может добавить в систему операторов, которые, в свою очередь, не будут иметь возможность изменять параметры и настройки ПК «Ребус-СОВ», но смогут наряду с администратором выполнять работу по аудиту событий ПК «Ребус-СОВ».

Настройка пользователей осуществляется в консоли управления во вкладке «Управление». Описание вкладки «Управление» и действий администратора по настройке пользователей приводится в разделе 4 ФДШИ.03618-01 34 01 «Руководство оператора».

4.7. Управление параметрами безопасности

Администратор должен осуществлять добавление и редактирование существующих правил для средства анализа сетевого трафика с использованием сигнатур и средства анализа

событий ОС и ПО. Любое изменение правил подразумевает задание переменных, использующихся в правилах, и редактирование/создание самих правил.

Заданные по умолчанию параметры могут быть изменены с использованием консоли управления СОВ, а также средства настройки агентской части СОВ. Наиболее критичными параметрами, влияющими на безопасность, являются:

- IP-адрес и порт сервера ПК «Ребус-СОВ»;
- параметры почтовой рассылки: IP-адрес почтового сервера, идентификатор и пароль пользователя, интервал рассылки;
- параметры архивирования событий аудита: максимальное количество событий в архиве, интервал смены архивов, интервал проверки свободного места, порог уведомления об отсутствии свободного места;
- параметры добавления нового пользователя СОВ: идентификатор, роль, пароль, электронная почта;
- параметры вывода событий аудита в SIEM: имя каталога для записи событий, адрес сервера для передачи событий,
- параметры автоматического обновления сигнатур вторжений из доверенных источников: интервал проверки наличия обновлений, IP-адрес и порт сервера обновлений, строковый идентификатор и пароль пользователя для подключения к серверу обновлений, путь к обновлению на сервере обновлений.

Данные параметры доступны только администратору СОВ. При вводе параметров в консоли управления осуществляется их проверка на правильность. Если параметр некорректный, то выводится предупреждающее сообщение и параметр не присваивается.

4.8. События безопасности

Описание каждого типа событий, относящихся к безопасности, а также событий, связанных с выполнением обязательных функций администрирования, приведено в 3.7.

4.9. Требования безопасности к среде функционирования

4.9.1. Общие требования безопасности к среде функционирования

Требования к среде функционирования изложены в разделе 2. Помимо функциональной настройки среды функционирования администратор безопасности должен выполнять настройку среды ИТ для обеспечения защиты программных модулей и данных ПК «Ребус-СОВ».

В состав функциональных требований безопасности входят:

- гарантии доступности данных аудита;
- обработка отказов аутентификации;
- верификация секретов;
- аутентификация до любых действий пользователей;
- идентификация до любых действий пользователей;
- невозможность обхода ПБО;
- отделение домена ФБО;
- тестирование абстрактной машины.

4.9.2. Гарантии доступности данных аудита

Администратор безопасности должен выполнять настройку средств разграничения доступа среды функционирования, запрещать доступ пользователей, не являющихся администраторами СОВ, к каталогам и файлам с записями аудита (расположение каталогов указано в 3.4). К серверу СОВ рекомендуется полностью запретить интерактивный доступ пользователей, не являющихся администраторами СОВ.

Пользователи СОВ должны получать доступ к записям аудита исключительно с использованием средств, предоставляемых ПК «Ребус-СОВ». ПК «Ребус-СОВ», в свою очередь, не позволяет пользователям выполнять модификацию и удаление записей аудита.

Администратор безопасности должен обеспечить безопасное хранение архивов, данных аудита в соответствии с требованиями системы защиты информации объекта. При передаче архивов с событиями на хранение необходимо обеспечить подсчет и хранение контрольных сумм файлов с архивами, а при анализе данных из архивов необходимо предварительно убедиться в том, что целостность файлов не нарушена, путем сравнения полученной контрольной суммы с контрольной суммой, сохраненной при передаче файлов с архивами событий на хранение. До передачи файлов с архивами на хранение целостность файлов контролируется средствами ПК «Ребус-СОВ».

При деинсталляции ПК «Ребус-СОВ» администратор безопасности должен убедиться, что все данные журналов ПК «Ребус-СОВ» были сохранены.

4.9.3. Обработка отказов аутентификации

Обработка отказов аутентификации должна выполняться средствами защиты уровня ОС.

СрЗИ уровня ОС должны противодействовать попыткам подбора аутентификационных данных злоумышленником. Для противодействия попыткам подбора:

- ЭВМ, на которых пользователям доступны средства управления СОВ, должны быть настроены на регистрацию событий ввода неверных аутентификационных данных;
- средства защиты должны быть настроены таким образом, чтобы при обнаружении нескольких неудачных попыток аутентификации предоставлять пользователю возможность выполнить аутентификацию только после истечения тайм-аута, выполнить перезагрузку ЭВМ, заблокировать учетную запись пользователя или заблокировать ЭВМ для пользователя.

Кроме того, обработка отказов аутентификации осуществляется средствами ПК «Ребус-СОВ». Аутентификация выполняется на сервере СОВ при доступе пользователя через консоль управления СОВ. При трех неудачных попытоках аутентификации, идущих подряд с одной станции, станция блокируется для дальнейшего подключения. Блокировка снимается автоматически через 1 минуту.

4.9.4. Верификация секретов

Администратор безопасности должен настроить механизм аутентификации СрЗИ уровня ОС на применение безопасных паролей. Пароль должен быть длиной не менее 6 – 8 буквенно-цифровых символов и соответствовать требованиям к паролям для класса ИС, в которой развернута СОВ. По возможности для генерации паролей должны применяться специальные датчики случайных чисел.

4.9.5. Аутентификация до любых действий пользователей

На ЭВМ, на которых предусмотрена интерактивная работа пользователей, в обязательном порядке должна выполняться аутентификация пользователей до начала работы пользователя. Аутентификация пользователей должна выполняться по буквенно-цифровому паролю длиной не менее 6 – 8 буквенно-цифровых символов и соответствовать требованиям к паролям для класса ИС, в которой развернута СОВ.

4.9.6. Идентификация до любых действий пользователей

На ЭВМ, на которых предусмотрена интерактивная работа пользователей, в обязательном порядке должна выполняться идентификация пользователей до начала работы пользователя. Авторизация пользователя в системе должна выполняться только после успешной идентификации и аутентификации. Неавторизованные пользователи не должны получать доступ к ИС. В процессе авторизации все процессы, выполняющиеся от имени пользователя, должны получать контекст

безопасности пользователя, на основании данного контекста СрЗИ уровня ОС должны принимать решения о предоставлении или отказе пользователю в доступе к ресурсам среды ИТ.

4.9.7. Невозможность обхода ПБО

Для обеспечения безопасности среды ИТ на ЭВМ необходимо использовать сертифицированные средства защиты от НСД.

4.9.8. Отделение домена ФБО

В частном случае операторы и администраторы СОВ могут являться пользователями и администраторами среды ИТ, в которой развернута СОВ. Данный случай актуален, когда область действия полномочий администратора среды ИТ и администратора СОВ совпадает.

В общем случае один домен СОВ может охватывать сразу несколько доменов безопасности среды ИТ. В данном случае невозможно выполнить совмещение учетных записей операторов и администраторов СОВ и пользователей ОС. Учетные записи операторов и администраторов СОВ создаются непосредственно в консоли управления СОВ. Учетные записи в среде ИТ создаются администраторами безопасности каждого из доменов безопасности. При создании учетных записей операторов и администраторов СОВ в среде ИТ администратор безопасности должен учитывать особые права данных пользователей к ресурсам СОВ и выполнять соответствующие настройки.

5. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

5.1. Входные данные

Входными данными для ПК «Ребус-СОВ» являются данные, собранные на агентских станциях, сигнатуры вторжений, настройки сетевых параметров, ключ для проведения аутентификации, команды пользователей.

5.2. Выходные данные

Выходными данными для ПК «Ребус-СОВ» являются сведения о выявленных вторжениях и реакции на них, статистика выявленных вторжений, сведения о состоянии компонентов СОВ, а также различные служебные сообщения.

ПРИЛОЖЕНИЕ 1

ОПИСАНИЕ СИГНАТУР ВТОРЖЕНИЙ

1. Формат сигнатур вторжений средства анализа сетевого трафика

Формат сигнатур вторжений средства анализа сетевого трафика совместим с форматом средства Snort. Сигнатуры содержатся в файлах с расширением **.rules**. Одна строка – одно правило. Комментарии в файлах **.rules** начинаются со знака «#», комментарии должны располагаться на отдельных строках, на строках с правилами комментариев быть не должно. Пустые строки игнорируются.

В таблице 1 данного приложения перечислены файлы ***.rules**, которые находятся в БРП на дистрибутивном ЭН и доступны сразу после установки.

Таблица 1 – Описание файлов с правилами

Файл	Назначение правил в файле
app-detect.rules	Правила обнаруживают определенные приложения, работающие в сети (например, Gizmo – аналог Skype)
browser-chrome.rules	Правила реагируют на проблемы соответствующих браузеров – переполнение адресной строки браузера, попытки отправить отчет об ошибках
browser-firefox.rules	
browser-ie.rules	
browser-other.rules	
browser-webkit.rules	
browser-plugins.rules	Правила регистрируют эксплуатацию уязвимостей в браузерных плагинах (например, flash)
content-replace.rules	Правила регистрируют подмену/компрометацию данных
emerging-activex.rules	Правила определяют использование вредоносных ActiveX-элементов
emerging-attack_response.rules	Правила срабатывают, когда локальный хост отправляет ответ, который похож на ответ подверженного атаке хоста
emerging-botcc.portgrouped.rules	Правила реагируют на трафик, схожий с тем, который генерирует C&C (Command&Control Centre) – центр управления ботнетом
emerging-botcc.rules	
emerging-chat.rules	Правила регистрируют использование чатов. Если в организации запрещено пользоваться программами мгновенного обмена сообщениями, то необходимо включить данный файл
emerging-ciarmy.rules	Правила регистрируют обращения к доменам из черного списка
emerging-compromised.rules	Правила регистрируют «опасные» запросы к удаленным ресурсам (попытка обращения к конфигурационным файлам web-сайтов вызывать cmd на удаленном узле и т.п.)
emerging-current_events.rules	Правила регистрируют активность вредоносного ПО
emerging-dns.rules	Правила реагируют на атаки, направленные на dns-серверы
emerging-dos.rules	Правила регистрируют DoS-атаки (в силу специфики таких атак правила вызывают много ложных срабатываний)
emerging-dshield.rules	Правила обнаруживают сетевой трафик от узлов, которые известны как источники атак на основе списка Dshield
emerging-drop.rules	Правила обнаруживают сетевой трафик от узлов из списка Spamhaus DROP list

Продолжение таблицы 1

Файл	Назначение правил в файле
emerging-exploit.rules	Правила реагируют на известные эксплоиты. Предупреждения генерируются в случае, если данными эксплоитами пытались воспользоваться, хотя сами эксплоиты к этому времени могли быть закрыты патчами или уязвимое ПО вообще может быть не установлено в системе
emerging-ftp.rules	Правила регистрируют атаки на ftp-серверы
emerging-games.rules	Правила реагируют на активность игровых приложений
emerging-icmp.rules	Правила обнаруживают сетевой трафик ICMP, характерного для проведения сетевых атак
emerging-icmp_info.rules	Правила реагируют на попытки пропинговать узлы сети с использованием некоторого хакерского инструментария, но учитывают любые пинги, которые могут в огромном количестве генерироваться вполне легитимным ПО
emerging-imap.rules	Правила регистрируют попытки атак на IMAP-серверы
emerging-inappropriate.rules	Правила регистрируют обращение к порнографическим материалам сети Интернет
emerging-info.rules	Правила реагируют на активность, которая может быть запрещена политикой безопасности в некоторых организациях. В отличие от emerging-policy.rules, правила реагируют на косвенные данные и нечеткие критерии, поэтому могут вызывать много ложных срабатываний
emerging-malware.rules	Правила регистрируют активность вредоносного ПО
emerging-misc.rules	Разные правила, не подпавшие под остальные категории
emerging-mobile_malware.rules	Правила регистрируют активность вредоносного ПО
emerging-netbios.rules	Правила регистрируют деятельность некоторых сетевых червей, атакующих машины под управлением Windows
emerging-p2p.rules	Правила регистрируют активность пиринговых программ, нарушающих законодательство (в частности, авторское право)
emerging-pop3.rules	Правила регистрируют потенциальные атаки на соответствующие почтовые службы
emerging-policy.rules	Правила реагируют на активность, которая может быть запрещена политикой безопасности в некоторых организациях (например, анонимный вход по ftp, запуск java-апплетов плееров для проигрывания видео, доступ к gmail и т.п.)
emerging-rpc.rules	Правила регистрируют атаки на службы удаленного вызова процедур
emerging-scada.rules	Правила регистрируют атаки из внешней сети на scada-системы
emerging-scan.rules	Правила регистрируют попытки сканирования сети. Содержат сигнатуры некоторых конкретных сетевых сканеров
emerging-shellcode.rules	Правила регистрируют в пересылаемых по сети пакетах шеллкод. Это, вероятнее всего, является легитимным трафиком
emerging-smtp.rules	Правила регистрируют потенциальные атаки на соответствующие почтовые службы

Продолжение таблицы 1

Файл	Назначение правил в файле
emerging-snmp.rules	Правила регистрируют несанкционированные попытки управления сетевым оборудованием по протоколу SNMP
emerging-sql.rules	Правила фиксируют атаки на SQL-серверы
emerging-telnet.rules	Правила информируют об опасном трафике, пересылаемом во время telnet-сессии
emerging-tftp.rules	Правила регистрируют потенциальные атаки на службы tftp
emerging-tor.rules	Правила регистрируют использование сети Tor
emerging-trojan.rules	Правила регистрируют работу вредоносного ПО
emerging-user_agents.rules	Правила регистрируют подозрительные параметры user-agent в web-трафике (использующиеся вредоносными web-ботами)
emerging-voip.rules	Правила регистрируют ошибки и потенциальные атаки на средства голосового общения по сети
emerging-web_client.rules	Правила регистрируют использование уязвимостей в web-клиентах
emerging-web_server.rules	Правила регистрируют использование уязвимостей в web-серверах
emerging-web_specific_apps.rules	Правила регистрируют использование уязвимостей в web-приложениях
emerging-worm.rules	Правила регистрируют активность вредоносного ПО
exploit-kit.rules	Правила предоставляют сигнатуры известных эксплоитов. Предупреждения генерируются в случае, если данными эксплоитами пытались воспользоваться, хотя сами эксплоиты к этому времени могли быть закрыты патчами или уязвимое ПО вообще может быть не установлено в системе
file-executable.rules	Правила информируют о наличии в пересылаемых по сети файлах потенциальной опасности (например, макросов в офисных документах)
file-flash.rules	
file-identify.rules	
file-image.rules	
file-java.rules	
file-multimedia.rules	
file-office.rules	
file-other.rules	
file-pdf.rules	
indicator-compromise.rules	Правила регистрируют опасные запросы к удаленным ресурсам (попытка обращения к конфигурационным файлам web-сайтов вызывать cmd на удаленном узле и т.п.)
indicator-scan.rules	Правила регистрируют попытки сканирования сети. Содержат сигнатуры некоторых конкретных сетевых сканеров
indicator-shellcode.rules	Правила регистрируют в пересылаемых по сети пакетах шеллкод. Это, вероятнее всего, является легитимным трафиком
malware-backdoor.rules	Правила реагируют на запрос соединения с удаленным компьютером, инициализированный вредоносным ПО

Продолжение таблицы 1

Файл	Назначение правил в файле
indicator-obfuscation.rules	Правила регистрируют в трафике обфусцированный JS-код. Как правило, его используют для защиты информации от автоматического копирования, но иногда с помощью него могут попытаться скрыть опасный код. Если такой трафик генерируется мало, то в принципе можно попытаться деобфусцировать полученные данные
malware-cnc.rules	Правила обнаруживают центр управления множеством компьютеров, реагируют на вредоносное ПО, ожидающее подключения новых ботов, регистрирующее их в своей базе, следящее за их состоянием и выдающее им команды, выбранные владельцем ботнета из списка всех возможных команд для бота
malware-other.rules	Правила регистрируют работу вредоносного ПО, не подпадающего под описание предыдущих двух пунктов
malware-tools.rules	Правила регистрируют работу хакерского инструментария на узле сети
netbios.rules	Правила регистрируют деятельность некоторых сетевых червей, атакующих машины под управлением Windows
os-linux.rules	Правила регистрируют эксплуатации уязвимостей в соответствующих ОС
os-mobile.rules	
os-other.rules	
os-solaris.rules	
os-windows.rules	
policy-multimedia.rules	Правила реагируют на активность, которая может быть запрещена политикой безопасности в некоторых организациях (например, анонимный вход по ftp, запуск java-апплетов плееров для проигрывания видео, доступ к gmail и т.п.)
policy-other.rules	
policy-social.rules	
policy-spam.rules	
protocol-dns.rules	Правила реагируют на атаки, направленные на dns-серверы
protocol-finger.rules	Правила регистрируют известные атаки на службу finger, которая по умолчанию запускается во многих unix-подобных ОС
protocol-ftp.rules	Правила регистрируют атаки на ftp-серверы
protocol-icmp.rules	Правила регистрируют попытки пропинговать узлы сети с использованием некоторого хакерского инструментария
protocol-imap.rules	Правила регистрируют попытки атак на IMAP-серверы
protocol-nntp.rules	Правила регистрируют атаки на службы времени
protocol-other.rules	Правила обнаруживают сетевой трафик, характерный для атак
protocol-pop.rules	Правила регистрируют попытки атак на POP-серверы
protocol-rpc.rules	Правила регистрируют атаки на службы удаленного вызова процедур
protocol-scada.rules	Правила регистрируют атаки из внешней сети на scada-системы
protocol-services.rules	Правила регистрируют команды удаленного доступа к системе (rlogin, rsh, rexec)
protocol-snmp.rules	Правила регистрируют активность SNMP-протокола (удаленное управление сетевым оборудованием)
protocol-telnet.rules	Правила информируют об опасном трафике, пересылаемом во время telnet-сессии

Окончание таблицы 1

Файл	Назначение правил в файле
protocol-tftp.rules	Правила регистрируют потенциальные атаки на службы tftp
protocol-voip.rules	Правила регистрируют ошибки и потенциальные атаки на средства голосового общения по сети
pua-adware.rules	Правила определяют активность adware-программ, которые нарушают права
pua-other.rules	Правила регистрируют возможные нарушения законодательства (использование Bitcoin, получение доступа к переписке)
pua-p2p.rules	Правила регистрируют активность пиринговых программ, нарушающих законодательство (в частности, авторское право)
pua-toolbars.rules	Правила определяют активность панелей инструментов, встраиваемых в браузер, нарушающих права (например, отправляющих статистику запросов на удаленный сервер без спроса пользователя)
scada.rules	Правила фиксируют атаки из внешней сети на scada-системы
server-apache.rules	Правила регистрируют эксплуатации уязвимостей в соответствующих серверах
server-iis.rules	
server-mail.rules	
server-mssql.rules	
server-mysql.rules	
server-oracle.rules	
server-other.rules	
server-samba.rules	
server-webapp.rules	
sql.rules	Правила регистрируют атаки на SQL-серверы
test.rules	Правила для самотестирования
x11.rules	Правила регистрируют потенциальные атаки, использующие уязвимости графического интерфейса UNIX-подобных ОС

Формат правил – ACTION PROTO IP_ADDR1 PORT1 DIRECTION IP_ADDR2 PORT2 (OPTIONS).

Поле ACTION определяет действие, выполняемое при срабатывании правила, может принимать одно из следующих значений:

- pass – ничего не делать;
- log – записать событие в журнал;
- alert – выдать предупреждение.

Поле PROTO задает сетевой протокол и может принимать одно из следующих значений:

- ip;
- icmp;
- tcp;
- udp.

Каждое из значений задает одноименный протокол.

Поле DIRECTION означает направление сетевого пакета и может принимать одно из следующих значений:

- «->» – правило действует только для пакетов, отправленных с IP_ADDR1 на IP_ADDR2;
- «<>» – правило действует для пакетов, проходящих в обоих направлениях.

Поле IP_ADDR – это IP-адрес. Может быть задан как в нотации IPv4, так и в нотации IPv6. Также можно указать ключевое слово «any», означающее любой адрес.

Поле PORT – номер порта из диапазона 0 – 64768. Может также использоваться ключевое слово «any».

Поле OPTIONS – список дополнительных параметров в скобках. Параметры разделяются точкой с запятой. Каждый параметр состоит из ключа и значения, разделенных двоеточием (например: msg: "MALWARE-BACKDOOR - Dagger_1.4.0").

В поле OPTIONS обязательно должны быть указаны следующие параметры:

1) описание события, обнаруживаемого данным правилом. Задается ключом msg;

2) идентификатор правила. Задается ключом sid;

3) класс вторжения, определяющий событие, которое будет зарегистрировано. Задается ключом classtype.

В правилах могут использоваться переменные. Формат объявления переменной следующий:

TYPE ID VALUE

Поле TYPE – тип переменной. Может принимать одно из следующих значений:

- var – текстовая переменная;
- ipvar – список IP-адресов;
- portvar – список сетевых портов.

Поле ID – идентификатор переменной. Может состоять из букв латиницы, цифр и знака подчеркивания «_». Не должен начинаться с цифры.

Поле VALUE – значение, которое присваивается переменной.

2. Формат сигнатур вторжений средства анализа событий ОС и прикладного ПО

Формат сигнатур вторжений средства анализа событий ОС и прикладного ПО совместим с форматом средства OSSEC.

Сигнатуры содержатся в файлах с расширением **xml**. Одно правило заключается в тег <rule>. Формат записи соответствует записи в стандартный xml-файл. Каждый xml-файл описывает правила для одного журнала.

Набор правил имеет древовидную структуру. Корневое правило должно описывать декодер, на основе которого обрабатываются сообщения из журнала. Конечные сработавшие правила содержат информацию, собранную всеми сработавшими правилами, начиная с корневого.

Набор правил имеет следующую структуру:

<group name=”имя_приложения,”>
    RULE
    ..
    RULE
</group>

Имя приложения не должно содержать пробелов и должно заканчиваться запятой. Оно должно кратко характеризовать приложение, журналы которого необходимо разобрать. Имя приложения является главной группой для всех событий из этого журнала.

Поле RULE описывает правило для данной группы. Количество правил не ограничивается.

Формат правил следующий:

<rule RULE_ATR>
    <RULE_TAG> .. </RULE_TAG>
</rule>

Поле RULE_ATR является атрибутом или списком атрибутов тега <rule>. Атрибуты данного поля представлены в таблице 2 данного приложения.

Таблица 2 – Набор атрибутов правила

Имя атрибута	Тип атрибута	Описание
id	Числовой, от 100 до 999999	Параметр определяет уникальный идентификатор правила
level	Числовой, от 0 до 15	Параметр определяет уровень угрозы
frequency	Числовой, количество	Параметр определяет частоту появления правила, на которое ссылается текущее правило, для его срабатывания
timeframe	Числовой, секунды	Параметр определяет временной интервал для атрибута frequency. Может быть использован только с атрибутом frequency

Поле RULE_TAG является внутренним тегом или набором внутренних тегов. Список внутренних тегов представлен в таблице 3 данного приложения.

Таблица 3 – Набор параметров правила

Имя тега	Тип атрибута	Описание
decoded_as	Текстовый	Параметр определяет имя декодера
description	Текстовый	Параметр определяет краткое описание события
if_sid	Числовой, идентификатор правила	Параметр определяет указатель на идентификатор правила, сработавшего ранее
match	Текстовый	Параметр определяет строку, при которой правило срабатывает, если в событии есть прямое совпадение с текстом внутри данной строки
regex	Текстовый, регулярное выражение	Параметр определяет строку с регулярным выражением, при которой правило срабатывает, если в событии есть совпадение по шаблону регулярного выражения
group	Текстовый	Правило определяет имя группы, которое будет добавлено к результирующей информации о событии

В обновленных сигнатурах могут встретиться дополнительные атрибуты и теги.

3. Методика добавления журнала для дальнейшего анализа событий с помощью средства анализа событий ОС и прикладного ПО

Настройка производится через редактирование конфигурационного файла **ossec.conf**. В ОС Windows файл располагается по пути **%ProgramFiles%\CPS\rebus-sov\ossec-agent\ossec.conf**. В ОС МСВС, ОС СН «Astra Linux Special Edition» файл располагается по пути **/usr/local/ossec/etc/ossec.conf**. Чтобы отредактировать конфигурационный файл, требуются права администратора.

Конфигурационный файл имеет следующую структуру для определения анализируемых журналов:

```
<localfile >
        <location>LOG_PATH</location>
        <log_format>LOG_FORMAT</log_format>
</localfile >
```

Переменная LOG_PATH должна принимать полный путь до анализируемого журнала.

Переменная LOG_FORMAT должна принимать значение из таблицы 4 данного приложения.

Таблица 4 – Форматы журналов

Имя формата	Описание
syslog	Данный формат подходит для журналов с форматом, подобным формату журнала syslog. Помимо этого, данный формат используется для журналов, формат которых не поддерживается. Данный формат не подходит для журналов, сообщения которых записаны более чем одной строкой
eventlog	Данный формат подходит для журналов ОС Windows, имеющих формат eventlog
mysql_log	Данный формат подходит для журналов СУБД MySQL
postgresql_log	Данный формат подходит для журналов СУБД PostgreSQL
multi-line: NUMBER	Данный формат подходит для журналов, в которых одно событие разбивается на NUMBER строк

Чтобы добавить новый журнал, который необходимо анализировать, требуется найти последнюю строку, в которой содержится запись </localfile>, перейти на следующую строку и вставить блок по описанной выше структуре.

Изменения вступают в силу только после перезагрузки плагина «Анализатор событий ОС и ПО».

ПРИЛОЖЕНИЕ 2

НАСТРОЙКА МАРШРУТИЗАЦИИ ПАКЕТОВ В ОС СН «ASTRA LINUX SPECIAL EDITION» И ОС МСВС 5.0

Чтобы ЭВМ под управлением ОС СН «Astra Linux Special Edition» могла работать в качестве межсетевого шлюза, необходимо в файле **/etc/sysctl.conf** раскомментировать строку *«net.ipv4.ip_forward=1»*. Если такой строки нет, ее нужно добавить. После сохранения изменений в файле **/etc/sysctl.conf** необходимо выполнить команду **sysctl –p** от имени суперпользователя.

После этой настройки ЭВМ сможет работать в качестве шлюза, т. е. перенаправлять сетевые пакеты с одного своего сетевого интерфейса на другой.

Чтобы ЭВМ под управлением ОС МСВС могла работать в качестве межсетевого шлюза необходимо в конец файла **/etc/rc.d/rc** добавить строку *«echo “1”>>/proc/sys/net/ipv4/ip_forward»* и перезагрузить ЭВМ.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АПКЗИ – аппаратно-программный комплекс защиты информации
АРМ – автоматизированное рабочее место
БРП – база решающих правил
ИС – информационная система
ИТ – информационная технология
ЛВС – локальная вычислительная сеть
МСВС – мобильная система Вооруженных сил
НСД – несанкционированный доступ
ОС – операционная система
ОС СН – операционная система специального назначения
ПБО – политика безопасности объекта
ПК – программный комплекс
ПО – программное обеспечение
СОВ – система обнаружения вторжений
СрЗИ – средство защиты информации
СУБД – система управления базами данных
ФБО – функция безопасности объекта
ЭВМ – электронно-вычислительная машина
ЭН – электронный носитель

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ докумен-та*	*Входящий № сопрово-дительного докум. и дата*	*Подп.*	*Да-та*
	изменен-ных	*заменен-ных*	*новых*	*аннули-рованных*					