УТВЕРЖДЕН
ДБАР.62.01.12.000.181-01 13-ЛУ

ПК «СОВ «ПЛУТОН-М1.0»

Описание программы

ДБАР.62.01.12.000.181-01 13

Листов 53

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

Москва
2018

СОДЕРЖАНИЕ

1 Общие сведения 4
1.1 Обозначение и наименование программы 4
1.2 Языки программирования, на которых написана программа 4
2 Функциональное назначение 5
2.1 Назначение программы 5
2.1.1 Назначение ПС Сенсор 5
2.1.2 Назначение ПС СУС 5
2.2 Решаемые задачи и функции 5
2.2.1 Решаемые задачи и функции ПС Сенсор 5
2.2.2 Решаемые задачи и функции ПС СУС 7
2.3 Сведения о функциональных ограничениях на применение программы 8
2.3.1 Сведения о функциональных ограничениях на применение ПС Сенсор 8
2.3.2 Сведения о функциональных ограничениях на применение ПС СУС 9
3 Описание логической структуры 11
3.1 Используемые методы 11
3.2 Структура программы с описанием функций составных частей и связи между ними 11
3.2.1 Модуль «Графический пользовательский интерфейс» 11
3.2.2 Модуль «Захват и буферизация» 12
3.2.3 Модуль «Сигнатурный анализ» 12
3.2.4 Модуль «Эвристический анализ» 12
3.2.5 Модуль «Сбор статистики» 13
3.2.6 Модуль «Копирование пакетов» 13
3.2.7 Модуль «Аудит безопасности» 14
3.2.8 Модуль «Обогащение СИБ» 15
3.2.9 Модуль «Мониторинг состояний» 15
3.2.10 Модуль «Обновление» 16
3.2.11 Модуль «Хранение больших данных» 18
3.2.12 Модуль «Хранение мастер-данных» 18
3.2.13 Модуль «Хранение файлов» 19
3.2.14 Модуль «Выполнение команд» 20
3.2.15 Модуль «Передача и приём данных и команд» 21
3.2.16 Модуль «Уведомления» 21
3.2.17 Другие функции ПК СОВ 22
3.3 Логическая схема программы 22
3.4 Связи программы с другими программами 25
3.5 Алгоритмы программы 26
3.5.1 Алгоритм обнаружения КА 26
3.5.2 Алгоритм обучения 28
3.5.3 Алгоритм сбора статистики 30
3.5.4 Алгоритм аудита безопасности 31
3.5.5 Алгоритм мониторинга состояния и работоспособности 31
3.5.6 Алгоритм выполнения команд 32
3.5.7 Алгоритм автоматического обновления БКЦ 34
3.5.8 Алгоритм обновления (кроме справочных данных) 35
3.5.9 Алгоритм регистрации компонента 38

3.5.10 Алгоритм передачи данных 39
3.5.11 Алгоритм регистрации на сервере обновлений 40
3.5.12 Алгоритм смены статусов ПС Сенсор 41
3.5.13 Алгоритм смены статусов ПС СУС 43
4 Используемые технические средства 45
5 Вызов и загрузка 46
5.1 Вызов программы 46
5.2 Входные точки в программу 46
Перечень сокращений 47
Перечень терминов 49

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование программы

Наименование программы: Программный комплекс «Система обнаружения вторжений «Плутон-М1.0» (далее – ПК СОВ).

Обозначение программы: ДБАР.62.01.12.000.181-01.

ПК СОВ состоит из двух программных средств (ПС):

1) «Сенсор-Плутон-М1.0» (далее – ПС Сенсор) – программное средство, предназначенное для обнаружения компьютерных атак (далее – КА), сбора статистики сетевого трафика и информации о хостах контролируемой системы.

Обозначение ПС Сенсор: ДБАР.62.01.12.000.183-01.

2) «СУС-Плутон-М1.0» (далее – ПС СУС) – программное средство, предназначенное для управления ПС Сенсор и системными параметрами, информирования пользователей ПК СОВ о зафиксированных КА в режиме реального времени и вывода статистических данных за заданный интервал времени.

Обозначение ПС СУС: ДБАР.62.01.12.000.182-01.

1.2 Языки программирования, на которых написана программа

ПК СОВ написан на языках программирования C++ версии 11, Python версии 3.6, ECMAScript 5.

2 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 Назначение программы

2.1.1 Назначение ПС Сенсор

ПС Сенсор предназначено для:

– обнаружения компьютерных атак (КА) в сетях передачи данных и аномалий в действиях хостов контролируемой системы;

– накопления статистики сетевого трафика и данных профилей хостов контролируемой системы.

2.1.2 Назначение ПС СУС

ПС СУС предназначено для:

– выполнения анализа данных о КА и аномалиях действий хостов контролируемой системы;

– управления сенсорами.

2.2 Решаемые задачи и функции

2.2.1 Решаемые задачи и функции ПС Сенсор

ПС Сенсор выполняет следующие функции:

1) Регистрация и идентификация сетевых вторжений на основе анализа сетевого трафика, передаваемого по контролируемому каналу связи.

2) Сбор информации об операционных системах, распределённом программном обеспечении, учётных записях пользователей, сертификатах хостов контролируемой системы.

3) Накопление информации о выявленных сетевых вторжениях в автономном режиме при отсутствии связи с ПС СУС и передача накопленной информации при восстановлении связи.

4) Контроль свободного дискового пространства, архивирование и автоматическое удаление устаревшей информации при переполнении жёсткого диска.

5) Регистрация событий аудита безопасности.

6) Фиксация, передача и обеспечение гарантированной доставки на ПС СУС:

– данных зарегистрированных сетевых вторжений – событий информационной безопасности;

– статистических характеристик сетевого трафика, передаваемого по контролируемому каналу передачи данных;

– параметров функционирования технических и программных средств ПС Сенсор;

– данных аудита безопасности ПС Сенсор;

– копии трафика;

– данных о сетевых взаимодействиях узлов контролируемых систем;

– собранных данных о профилях хостов;

– данных о распределённом программном обеспечении узлов контролируемых систем.

7) Агрегация однотипных событий.

8) Предоставление пользователям возможности настроить ПС Сенсор и изменить его параметры конфигурирования с помощью командной среды операционной системы (ОС).

9) Выполнение команд, поступающих из ПС СУС.

10) Регулирование доступа пользователей к функциям ПС Сенсор в соответствии с настройками ролевой модели доступа. В поставке ПК СОВ предусмотрена роль «Администратор безопасности СОВ», которая даёт право на запуск команды настройки и конфигурирования ПС Сенсор с помощью командной среды ОС.

11) Идентификация, аутентификация и авторизация пользователей выполняется средствами операционной системы. При этом:

– для доступа используются логины и пароли пользователей;

– отслеживается выполнение требований к сложности пароля (длина, специальные символы, цифры, буквы в верхнем и нижнем регистре) и к периодичности смены пароля.

12) Взаимодействие ПС Сенсор с ПС СУС по защищённому каналу связи. Для исключения несанкционированного доступа во время установки соединения удалённый компонент идентифицируется с помощью проверки цифрового сертификата.

13) Обновление ПС Сенсор в части базы решающих правил сигнатурного анализа, чёрных списков, программных сценариев эвристического анализа, справочников, базы уязвимости, базы GeoIP и программного обеспечения.

14) Маскирование своего функционирования за счёт применения механизмов операционной системы.

2.2.2 Решаемые задачи и функции ПС СУС

ПС СУС выполняет следующие функции:

1) Поддержка иерархической модели подчинения компонентов ПС СУС и ПС Сенсор.

2) Предоставление пользователю возможности анализировать данные: как поступающих с подчинённых компонентов, так генерируемых самим ПС СУС с помощью графического пользовательского интерфейса.

3) Приём от ПС Сенсор, хранение и передача на вышестоящий ПС СУС:

– СИБ;

– статистических характеристик сетевого трафика, передаваемого по контролируемому каналу передачи данных;

– параметров функционирования технических и программных средств – своих и подчинённых компонентов;

– данных аудита безопасности – своих и подчинённых компонентов;

– копий трафика;

– данных о распределённом программном обеспечении узлов контролируемых систем;

– профилей хостов.

4) Импорт информации о профилях хостов контролируемых систем и передача их на ПС Сенсор.

5) Регистрация событий аудита безопасности.

6) Предоставление пользователям возможности настроить ПС СУС и подчинённые компоненты и изменить параметры их конфигураций с помощью командной среды ОС и графического пользовательского интерфейса.

7) Выполнение команд, поступающих из вышестоящего ПС СУС.

8) Регулирование доступа пользователей к функциям ПС СУС в соответствии с настройками ролевой модели доступа. В поставке ПК СОВ предусмотрены:

– роль «Администратор безопасности СОВ», которая даёт право настраивать ПС СУС и подчинённые компоненты и изменять параметры конфигураций с помощью командной среды ОС и графического пользовательского интерфейса;

– роль «Оператор визуального контроля СОВ», которая даёт право:

a) анализировать СИБ,

b) анализировать собственные события аудита безопасности и события аудита безопасности подчинённых компонентов

c) анализировать собственное состояние и состояние подчинённых компонентов

d) настраивать решающие правила сигнатурного анализа.

9) Идентификация, аутентификация и авторизация пользователей выполняется через механизмы операционной системы. При этом:

– для доступа используются логины и пароли пользователей;

– отслеживается выполнение требований к сложности пароля (длина, специальные символы, цифры, буквы в верхнем и нижнем регистре) и к периодичности смены пароля.

10) Взаимодействие программных средств ПК СОВ по защищённому каналу связи. Для исключения несанкционированного доступа во время установки соединения удалённый компонент идентифицируется с помощью проверки цифрового сертификата.

11) Взаимодействие с внешней системой обновлений.

12) Обновление ПС СУС в части базы решающих правил сигнатурного анализа, чёрных списков, справочников, базы уязвимости, базы GeoIP, данных картографии, программного обеспечения и передача обновлений на подчинённые компоненты.

13) Предоставление данных СИБ в формате CEF (Common Event Format) для передачи во внешние SIEM-системы.

2.3 Сведения о функциональных ограничениях на применение программы

2.3.1 Сведения о функциональных ограничениях на применение ПС Сенсор

2.3.1.1 ПС Сенсор функционирует на ЭВМ с характеристиками производительности не ниже, чем ЭВМ архитектуры x86-64, оснащённой сетевыми интерфейсами, поддерживающими скорость передачи данных до 10 Гбит/с.

2.3.1.2 Для установки и функционирования ПС Сенсор требуется свободное пространство на жёстком диске ЭВМ объёмом не менее 50 Гб.

2.3.1.3 ПС Сенсор функционирует под управлением ОС Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2.3.1.4 Формат и метод кодирования сетевых пакетов в контролируемом канале передачи данных должны соответствовать стандарту RFC 791.

2.3.1.5 Для обеспечения маскирования работы сенсора сетевой интерфейс, используемый для захвата контролируемого сетевого трафика, должен работать в режиме прослушивания трафика и не должен создавать исходящий трафик в контролируемую систему.

2.3.1.6 В случае подключения сетевого интерфейса сенсора в разрыв контролируемого трафика, для обеспечения функционирования контролируемой системы при наступлении нештатного или аварийного состояния сетевого интерфейса, сетевой интерфейс должен обеспечивать работу в режиме bypass. Режим bypass обеспечивает сетевой интерфейс с одним основным и одним обводным (байпас) портом. Переключение основного порта на байпас порт происходит автоматически.

2.3.1.7 Для обеспечения защиты процессов взаимодействия ПС Сенсор и ПС СУС во время установки соединения удалённый компонент должен идентифицироваться с помощью проверки цифрового сертификата.

2.3.1.8 ЭВМ, на которую устанавливается ПС Сенсор, должна размещаться в условиях закрытых отапливаемых и кондиционируемых помещений, снабжённых необходимыми средствами пожарной безопасности.

2.3.1.9 ЭВМ должна быть обеспечена бесперебойным электропитанием.

2.3.1.10 Физический доступ в помещение, где функционирует ПС Сенсор, должен быть ограничен.

2.3.1.11 Доступ к ПС Сенсор и право работы на нем должны иметь только зарегистрированные пользователи.

2.3.2 Сведения о функциональных ограничениях на применение ПС СУС

2.3.3 ПС СУС функционирует на ЭВМ с характеристиками производительности не ниже, чем ЭВМ архитектуры x86-64, оснащённой сетевыми интерфейсами, поддерживающими скорость передачи данных до 1 Гбит/с.

2.3.4 Для установки и функционирования ПС СУС требуется свободное пространство на жёстких магнитных дисках, объединённых в RAID-массив объёмом не менее 24 Тбайт.

2.3.5 ПС СУС функционирует под управлением ОС Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2.3.6 ЭВМ, на которую устанавливается ПС СУС, должна размещаться в условиях закрытых отапливаемых и кондиционируемых помещений, снабжённых необходимыми средствами пожарной безопасности.

2.3.7 ЭВМ должна быть обеспечена бесперебойным электропитанием.

2.3.8 Физический доступ в помещение, где функционирует ПС СУС, должен быть ограничен.

2.3.9 Доступ к ПС СУС и право работы на нем должны иметь только зарегистрированные пользователи.

3 ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1 Используемые методы

3.1.1 Обнаружение сетевых вторжений в ПС Сенсор выполняется с помощью сигнатурного метода обнаружения компьютерных атак (КА), который сводится к поиску в сетевых пакетах уникальных последовательностей (сигнатур). Такие сигнатуры однозначно определяют КА. Поиск выполняется путём проверок заголовков и содержимого сетевых пакетов на соответствие условиям, заданным решающими правилами сигнатурного анализа. В ПС Сенсор используются сигнатурные правила СОА Suricata, СОА Bro и утилиты p0f.

3.1.2 Обнаружение подозрительной активности в ПС Сенсор выполняется с помощью метода поиска по чёрным спискам. С помощью чёрных списков в сетевом трафике обнаруживаются подозрительные IP-адреса, адреса электронной почты, DNS-имена, URL-адреса, MD5-хешы подозрительных файлов. Чёрные списки хранятся в БД ПС Сенсор.

3.1.3 Обнаружение аномалий действий хостов контролируемой системы в сети передачи данных выполняется методом статистического анализа. ПС Сенсор собирает статистические характеристики потоков трафика в контролируемом канале передачи данных. Полученные данные агрегируются и в дальнейшем используются для выявления аномалий. Метод статистического анализа позволяет выявлять сетевые вторжения, осуществляемые заранее неизвестным способом и/или не имеющие характерных сигнатур.

3.2 Структура программы с описанием функций составных частей и связи между ними

ПК СОВ состоит из модулей:

3.2.1 Модуль «Графический пользовательский интерфейс»

Модуль представляет собой веб-приложение, работающее в среде браузера и защищённое протоколом HTTPS. Модуль предоставляет графический пользовательский интерфейс (ГПИ) к функциям ПС СУС и позволяет:

– просматривать, фильтровать и проводить поиск данных о СИБ, событиях аудита безопасности;

– просматривать статистику контролируемого сетевого трафика в виде графиков и диаграмм;

– просматривать данные мониторинга компонентов, профилей хостов, топологии сети;

– просматривать КА и местоположение объектов ПК СОВ на географической карте;

– просматривать решающие правила сигнатурного анализа и чёрные списки;

– выполнять настройки компонентов ПК СОВ и параметров контролируемых систем;

– управлять пользователями ПС СУС и настраивать ролевую модель доступа;

– инициировать команды регистрации компонентов, активирования/деактивирования компонентов и решающих правил сигнатурного анализа и чёрных списков, подтверждения данных профиля хоста.

3.2.2 Модуль «Захват и буферизация»

Модуль выполняет захват и кольцевую буферизацию сетевого трафика помощью программного интерфейса операционной системы в ПС Сенсор. Сенсор может работать в режимах:

– разрыв канала;

– прослушивание канала (использует копию сетевого трафика).

Входная информация: сетевой трафик.

Выходная информация: захваченные пакеты сетевого трафика.

3.2.3 Модуль «Сигнатурный анализ»

Модуль выполняет сигнатурный анализ пакетов сетевого трафика, формирует СИБ и журналы событий.

Правила сигнатурного анализа хранятся в виде файлов. Хранение данных обеспечивает модуль «Хранение файлов».

Входная информация: захваченные пакеты сетевого трафика, база решающих правил сигнатурного анализа.

Выходная информация: сырые данные СИБ.

3.2.4 Модуль «Эвристический анализ»

Модуль:

– выявляет новые хосты в контролируемой системе;

– выявляет новое ПО на хостах контролируемой системы;

– обнаруживает в сетевом трафике те атрибуты сущностей, которые включены в чёрные списки;

– в режимах обучения и обнаружения КА собирает данные о профилях хостов контролируемой системы.

Программные сценарии эвристического анализа хранятся в виде файлов. Хранение данных обеспечивает модуль «Хранение файлов».

Входная информация: пакеты сетевого трафика.

Выходная информация: сырые данные СИБ, данные профилей хостов.

3.2.5 Модуль «Сбор статистики»

Модуль выполняет сбор статистики пакетов сетевого трафика с учётом входящих/исходящих потоков данных с разделением по хостам контролируемой системы ПС Сенсор, по портам и протоколам. Собранная статистика используется для анализа аномалий действий хостов контролируемой системы. Данные статистики хранятся в БД ПС Сенсор. Хранение обеспечивает модуль «Хранение больших данных» (см. раздел 3.2.11).

Входная информация: захваченные пакеты сетевого трафика.

Выходная информация: статистика, события статистики.

3.2.6 Модуль «Копирование пакетов»

Для СИБ модуль создаёт копию трафика в виде PCAP-файла[1)]. PCAP-файл содержит информацию: о сетевом пакете, вызвавшем срабатывание решающего правила и десяти пакетах после этого пакета – при их наличии в сетевом соединении. Дополнительная информация для СИБ расширяет возможности расследования СИБ. Хранение копий пакетов обеспечивает модуль «Хранение файлов» (см. раздел 3.2.13).

Входная информация: захваченные пакеты сетевого трафика.

Выходная информация: PCAP-файлы.

---

1) PCAP-файл создаётся только для сигнатурных событий Suricata

3.2.7 Модуль «Аудит безопасности»

Модуль предназначен для выполнения контролирующих действий и регистрации событий ПС ПК СОВ, которые потенциально могут быть опасными для работоспособности ПС ПК СОВ.

Модуль выполняет:

– аудит целостности, при котором выявляются несанкционированные изменения объектов ПС ПК СОВ (ПО, конфигурационные файлы, база решающих правил сигнатурного анализа, чёрные списки, программные сценарии эвристического анализа);

– аудит действий пользователей ПК СОВ;

– аудит изменений режимов работы ПС ПК СОВ;

– аудит выполнение программ и процессов ПС ПК СОВ.

Аудит целостности использует базу контроля целостности (БКЦ), которая содержит контрольные суммы объектов ПС ПК СОВ. Хранение БКЦ обеспечивает модуль «Хранение файлов» (см. раздел 3.2.13).

Модуль выполняет аудит целостности ПС ПК СОВ:

– при старте ПС ПК СОВ;

– по расписанию в соответствии с установленными временными интервалами;

– по команде администратора безопасности СОВ.

Модуль инициирует уведомление пользователей ПК СОВ о событиях аудита. Уведомления формируются и отправляются на адреса электронной почты пользователей в соответствии с настройками (см. раздел 3.2.16).

Модуль выполняет обновление БКЦ. Алгоритм обновления БКЦ представлен в разделе 3.5.7.

К событиям аудита безопасности относятся:

– запуск и завершение выполнения функций аудита безопасности;

– запуск и завершения самотестирования;

– запуск и завершение программ и процессов ПК СОВ;

– изменение режимов выполнения функций ПК СОВ;

– попытка удаления СИБ и событий аудита безопасности;

– вход и выход пользователей ПК СОВ;

– неуспешные попытки входа пользователей ПК СОВ;

– изменение настроек ролевой модели доступа к функциям ПК СОВ;

– изменение учётной записи пользователя и изменение пароля пользователя;

– изменение полномочий пользователей ПК СОВ.

Хранение событий аудита безопасности в БД ПС ПК СОВ обеспечивает модуль «Хранение больших данных» (см. раздел 3.2.11).

Входная информация: БКЦ, события обучения, мониторинга состояния, обновлений, выполнения команд.

Выходная информация: события аудита безопасности ПС ПК СОВ, БКЦ.

3.2.8 Модуль «Обогащение СИБ»

Модуль предназначен для буферизации и обогащения сырых данных СИБ дополнительной информацией, которая содержится:

– в базах решающих правил сигнатурного анализа;

– в чёрных списках;

– в профилях хостов;

– в справочниках,

– в базе уязвимостей,

– в базе GeoIP.

Входная информация: сырые данные СИБ, база решающих правил сигнатурного анализа, черные списки, профили хостов, справочники, база уязвимостей, база GeoIP.

Выходная информация: СИБ.

3.2.9 Модуль «Мониторинг состояний»

Модуль отслеживает состояние и работоспособность ПС ПК СОВ, а также выполняет самотестирование работоспособности ПС ПК СОВ:

– при старте ПС ПК СОВ;

– по расписанию в соответствии с установленными временными интервалами;

– по команде администратора безопасности СОВ.

Показатели состояния и работоспособности сохраняются в БД ПС ПК СОВ. Для хранения используется модуль «Хранение мастер-данных» (см. раздел 3.2.12).

Данные мониторинга используются для определения следующих показателей работоспособности:

- процент использования ОЗУ;
- процент использования ЦПУ;
- процент использования файла подкачки;
- процент использования НЖМД;
- признак компрометации ПС ПК СОВ.

Входная информация: пороговые значения.

Выходная информация: показатели состояния ПС ПК СОВ, события мониторинга.

3.2.10 Модуль «Обновление»

Модуль выполняет обновление и импорт в БД ПС ПК СОВ обновлённой информации.

Обновление некорневого ПС СУС.

Модуль отслеживает публикации обновлений в вышестоящем ПС СУС. При наличии обновлений модуль скачивает сжатые файлы обновлений (за исключением справочников) и распаковывает их.

Модуль устанавливает файлы обновлений:

- базы GeoIP;
- данных картографии;
- программного обеспечение ПС СУС.

Хранение данных обеспечивает модуль «Хранение файлов».

Модуль импортирует данные следующих обновлений в БД ПС СУС:

- база решающих правил сигнатурного анализа;
- чёрные списки;
- база уязвимости.

Хранение импортируемых данных обеспечивает модуль «Хранение мастер-данных» (см. раздел 3.2.12).

Алгоритм обновления представлен в разделе 3.5.8.

Обновление справочных данных выполняет модуль «Передача и приём данных и команд». Справочные данные передаются из БД вышестоящего ПС СУС в БД ПС СУС..

Обновление корневого ПС СУС.

Модуль выполняет регистрацию на сервере обновлений (см. раздел 3.5.11) и проводит мониторинг публикации обновлений на сервере обновлений посредством HTTP-запросов. При наличии обновлений модуль скачивает сжатые файлы обновлений (за исключением справочников) и распаковывает их.

Модуль устанавливает файлы обновлений:

- базы GeoIP;
- данных картографии;
- программного обеспечение ПС СУС.

Хранение данных обеспечивает модуль «Хранение файлов».

Модуль импортирует данные следующих обновлений в БД ПС СУС:

- база решающих правил сигнатурного анализа;
- чёрные списки;
- база уязвимости.

Хранение импортируемых данных обеспечивает модуль «Хранение мастер-данных» (см. раздел 3.2.12).

Обновление ПС Сенсор

Модуль отслеживает публикации обновлений в ПС СУС и при наличии обновлений скачивает сжатые файлы обновлений (за исключением справочников) и распаковывает их.

Модуль устанавливает файлы обновлений:

- базы решающих правил сигнатурного анализа;
- чёрных списков;
- программных сценариев эвристического анализа;
- базы GeoIP;
- программного обеспечение ПС Сенсор.

Хранение данных обеспечивает модуль «Хранение файлов».

Модуль импортирует данные следующих обновлений в БД ПС Сенсор:

– база решающих правил сигнатурного анализа;

– чёрные списки;

– база уязвимости.

Хранение импортируемых данных обеспечивает модуль «Хранение мастер-данных» (см. раздел 3.2.12).

Обновление справочных данных

Обновление справочных данных выполняет модуль «Передача и приём данных и команд». Справочные данные передаются из БД ПС СУС в БД подчинённого компонента.

Алгоритм обновления представлен в разделе 3.5.8.

Входная информация: файлы обновлений, справочники.

Выходная информация: установленное ПО, обновлённые база уязвимостей, решающие правила сигнатурного анализа, чёрные списки, программные сценарии эвристического анализа, база GeoIP, данные картографии, справочники, события обновлений, импортированные в БД ПС ПК СОВ база решающих правил сигнатурного анализа, чёрные списки, база уязвимостей.

3.2.11 Модуль «Хранение больших данных»

Модуль используется для хранения следующих видов данных:

– СИБ;

– журналы событий;

– события аудита безопасности;

– статистика сетевого трафика.

Модуль поддерживает функции:

– резервного копирования БД по расписанию или по команде администратора безопасности СОВ;

– восстановление данных БД из резервной копии;

– архивирование;

– удаление исторических данных.

3.2.12 Модуль «Хранение мастер-данных»

Модуль используется для хранения следующих видов данных:

– профили хостов;

– база решающих правил сигнатурного анализа;

– чёрные списки;

– справочники;

– база уязвимостей.

Модуль поддерживает функции:

– резервного копирования БД по расписанию или по команде администратора безопасности СОВ;

– восстановление данных БД из резервной копии;

– архивирование;

– удаление исторических данных.

3.2.13 Модуль «Хранение файлов»

Модуль решает задачи хранения в файловой системе ОС ПС ПК СОВ:

– файлов решающих правил сигнатурного анализа (только для ПС Сенсор);

– файлов чёрных списков (только для ПС Сенсор);

– файлов программных сценариев эвристического анализа (только для ПС Сенсор);

– PCAP-файлов;

– файлов базы GeoIP;

– файлы данных картографии (только для ПС СУС);

– файлов обновлений.

Модуль поддерживает функции:

– резервного копирования по расписанию или по команде администратора безопасности СОВ;

– восстановление данных из резервной копии;

– архивирование;

– удаление исторических данных.

3.2.14 Модуль «Выполнение команд»

Модуль обеспечивает выполнение команд, которые инициируются:

– из командной среды ОС ПС ПК СОВ;

– из модуля «Графический пользовательский интерфейс» ПС СУС.

Передачу команд от одного компонента к другому компоненту выполняет модуль «Передача и приём данных и команд» (см. раздел 3.2.15).

В таблице 1 представлен перечень команд:
Таблица 1 – Перечень команд ПК СОВ

Команда	**ГПИ**	**Командная среда ОС**
Регистрация компонента	Да	Да
Регистрация на сервере обновлений	Да	
Изменение статуса компонента	Да	
Активирование/деактивирование решающих правил сигнатурного анализа	Да	
Подтверждение профиля хоста	Да	
Подтверждение ПО хоста	Да	
Запуск обновления базы контроля целостности	Да	
Запуск контроля целостности	Да	
Установка параметров контролируемой системы	Да	
Создание резервных копий БД ПК СОВ		Да
Восстановление данных из резервных копий БД ПК СОВ		Да
Установка значений параметров в конфигурационных файлах: – пороговые значения статистического анализатора; – параметры архивирования и удаления исторических данных; – параметры выполнения процедуры предотвращения переполнения НЖМД; – параметры выполнения процедуры самотестирования; – параметры формирования уведомлений; – параметры агрегации однотипных СИБ		Да

Входная информация: команды.

Выходная информация: результаты выполнения команд.

3.2.15 Модуль «Передача и приём данных и команд»

Модуль обеспечивает взаимодействие ПС ПК СОВ. Для реализации функций модуля используется протокол MQTT. Используется шаблон взаимодействия публикации/подписки. Взаимодействие ПС ПК СОВ осуществляется по защищённому каналу связи. Для исключения несанкционированного доступа модуль во время установки соединения идентифицирует удалённый компонент с помощью проверки цифрового сертификата.

Модуль обеспечивает передачу данных:

- из вышестоящего компонента в подчинённый компонент:
  - файлы обновлений;
  - справочники;
  - профили хостов (только от ПС СУС в подчинённое ПС Сенсор).
- из подчинённого компонента в вышестоящий компонент:
  - СИБ;
  - журналы событий;
  - PCAP-файлы;
  - события аудита безопасности подчинённых компонентов;
  - статистика трафика;
  - профили хостов;
  - состояния подчинённых компонентов.

Модуль обеспечивает приём команд, представленный в разделе 3.2.14.

Программный интерфейс взаимодействия компонентов ПК СОВ предоставляется в виде сервисов на стороне ПС СУС. За счёт этого достигнута независимость от реализации клиентов на стороне ПС Сенсор. Формат и структура данных спроектированы таким образом, чтобы обеспечить возможность лёгкого расширения.

3.2.16 Модуль «Уведомления»

Модуль выполняет рассылку уведомлений пользователям ПК СОВ по электронной почте. Рассылка запускается по факту появления СИБ в ПС Сенсор и событий аудита безопасности в ПС ПК СОВ. Можно выбрать следующие настройки уведомлений:

- формирование уведомлений в зависимости от типа события;

– формирование уведомления в зависимости от уровня критичности события;

– формирование списков рассылки.

Входная информация: СИБ, сообщения аудита безопасности

Выходная информация: сообщения электронной почты.

Используемые сервисы:

– pluton-notification-server.

3.2.17 Другие функции ПК СОВ

ПК СОВ включают в себя сервисы, программные сценарии, команды, реализующие отдельные функции:

– Сервис pluton-job-runner поддерживает запуск процессов ПК СОВ по расписанию.

– Сервис pluton-homenet-control реализует применение параметров контролируемой системы в ПС Сенсор.

– Сервис pluton-service-start реализует запуск процессов ПК СОВ, работающих в фоновом режиме.

– Программный сценарий remove_oldest_data.sh по команде модуля «Мониторинг состояний» выполняет действия, предотвращающие переполнение дискового пространства компонента ПК СОВ.

– Интерфейс командной строки (CLI) pluton [options] выполняет команды, которые используются ПК СОВ и могут быть использованы для выполнения команд из командной строки ОС. С помощью интерфейса командной строки можно:

а) выполнять резервное копирование и восстановление БД ПК СОВ;

б) запускать программный сценарий remove_oldest_data.sh;

в) управлять локальными пользователями ОС;

г) импортировать профили хостов.

– Сервис pluton-ise-handler на основе данных о СИБ формирует сообщение в формате CEF (Common Event Format) для внешних SIEM-систем.

3.3 Логическая схема программы

В таблице 2 представлена информация о применении модулей ПК СОВ в ПС Сенсор и ПС СУС.

Таблица 2 – Применение модулей ПК СОВ в программных средствах

Модуль	**ПС Сенсор**	**ПС СУС**
Захват и буферизация	Да	
Сигнатурный анализ	Да	
Эвристический анализ	Да	
Сбор статистики	Да	
Копирование пакетов	Да	
Обогащение СИБ	Да	
Графический пользовательский интерфейс		Да
Аудит безопасности	Да	Да
Мониторинг состояний	Да	Да
Выполнение команд	Да	Да
Обновление	Да	Да
Уведомления	Да	Да
Хранение больших данных	Да	Да
Хранение мастер-данных	Да	Да
Хранение файлов	Да	Да
Передача и приём данных и команд	Да	Да

На рисунке 1 представлена логическая схема ПС Сенсор.

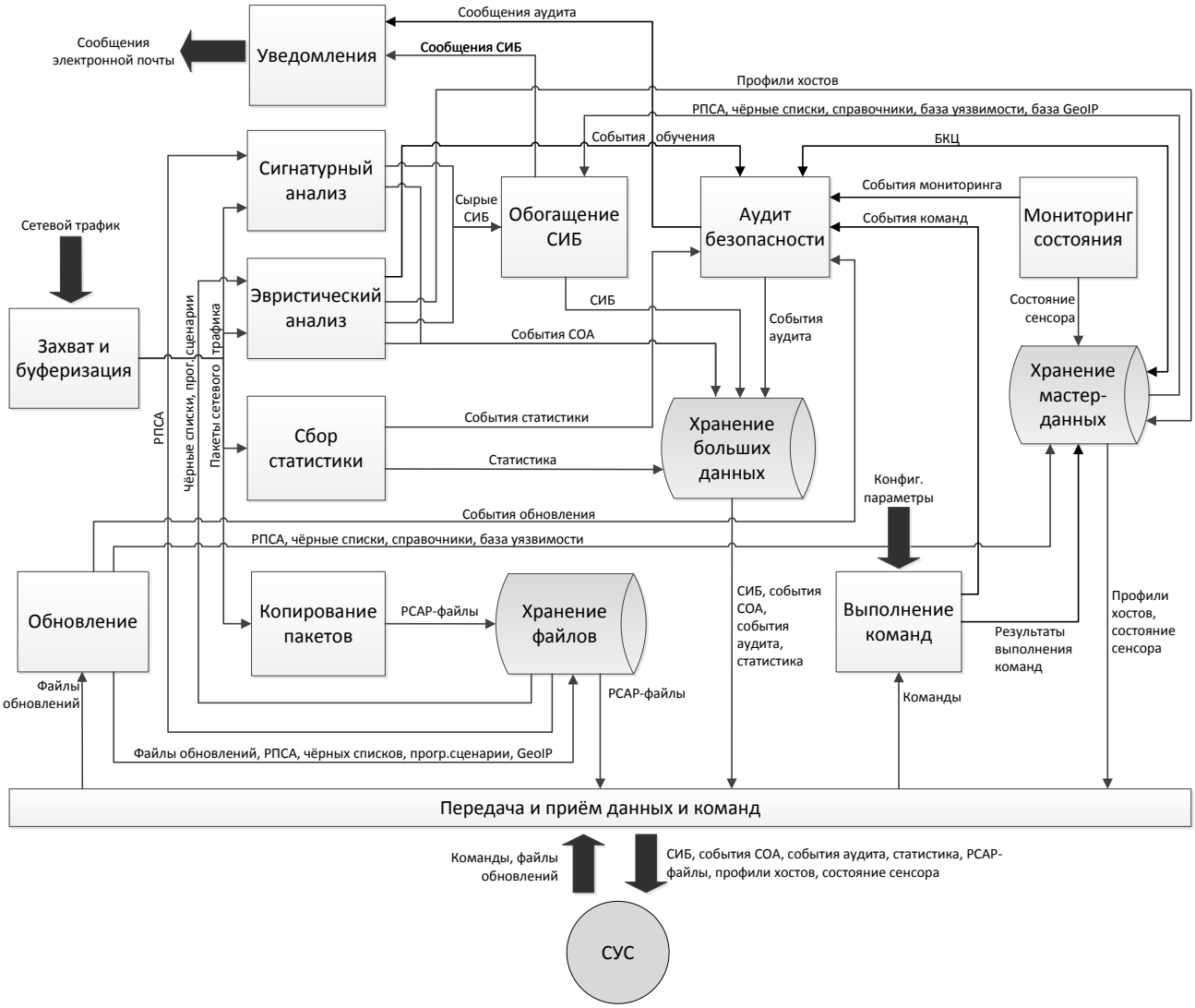

Рисунок 1 – Логическая схема ПС Сенсор

На рисунке 2 представлена логическая схема ПС СУС.

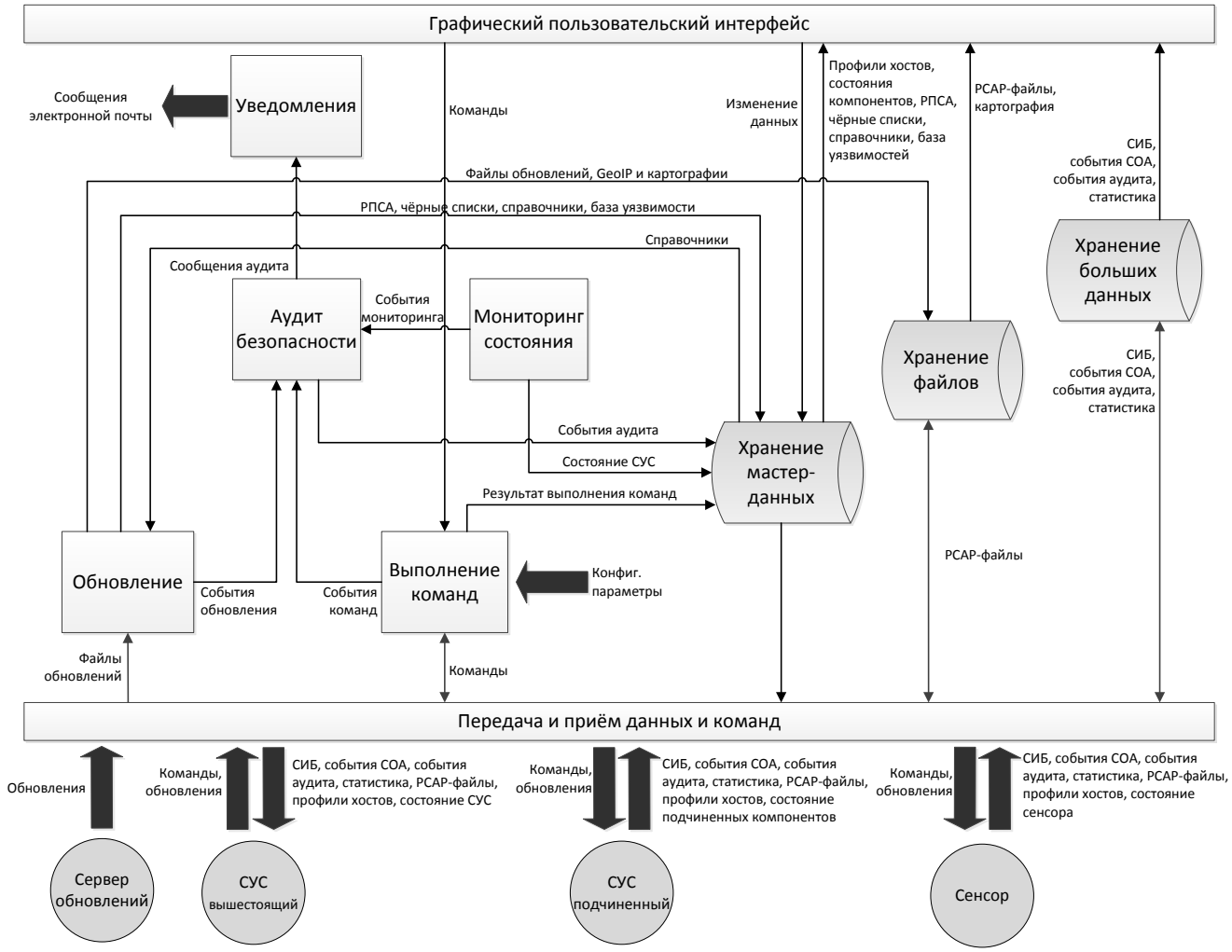

Рисунок 2 – Логическая схема ПС СУС

3.4 Связи программы с другими программами

ПК СОВ взаимодействует с сервером обновлений, который является источником обновлений:

- базы решающих правил сигнатурного анализа;
- чёрных списков;
- программных сценариев эвристического анализа;
- справочников;
- базы уязвимости;
- базы GeoIP;

– данных картографии;

– программного обеспечения ПС ПК СОВ.

Взаимодействие ПК СОВ с севером обновлений происходит:

– во время регистрации компонента ПК СОВ на сервере обновлений (см. раздел 3.5.11);

– во время передачи обновлений с сервера обновлений в ПС СУС (см. раздел 3.5.8).

Взаимодействие ПК СОВ с сервером обновлений осуществляется по защищённым каналам связи.

3.5 Алгоритмы программы

3.5.1 Алгоритм обнаружения КА

На рисунке 3 представлена блок-схема алгоритма обнаружения КА.

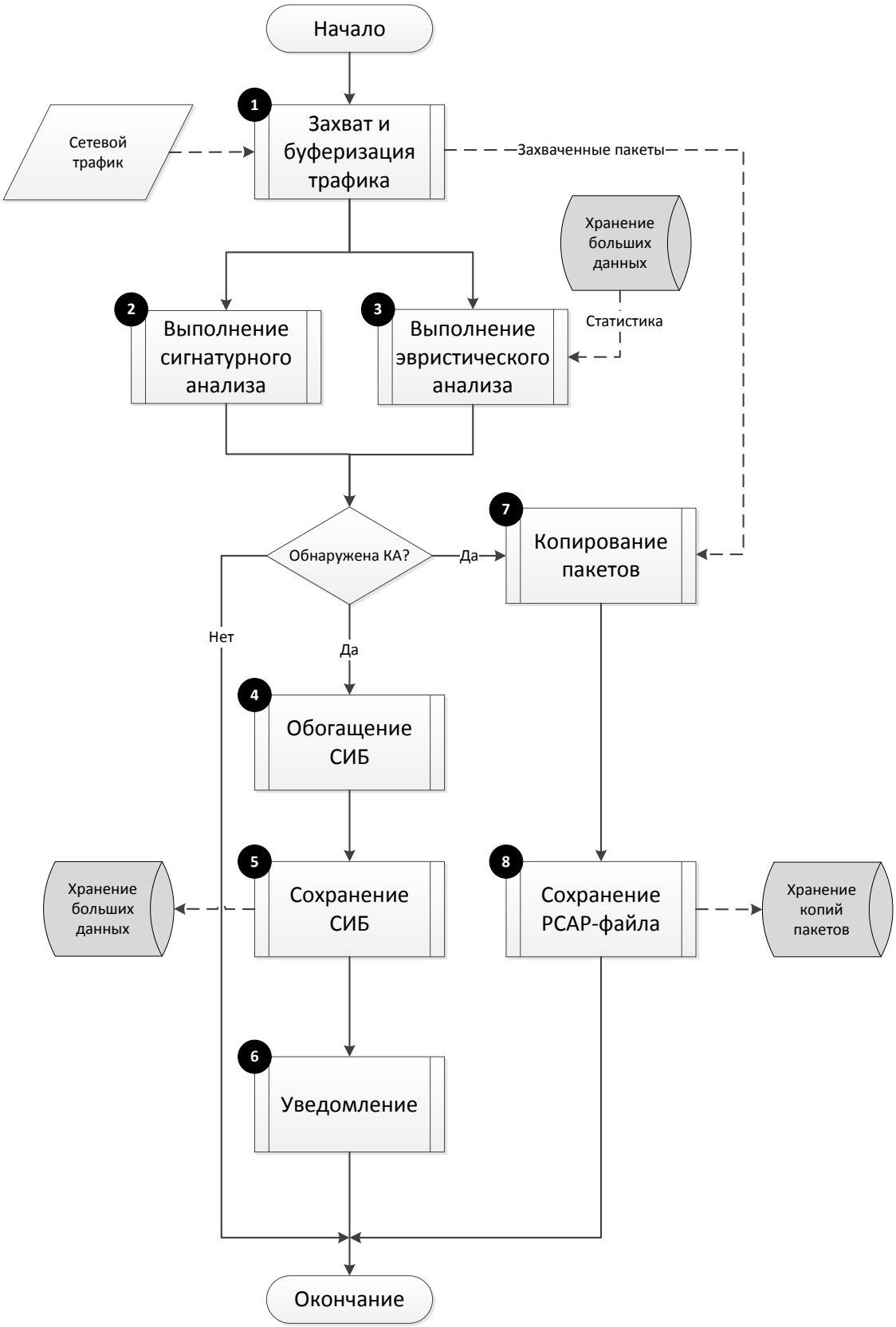

Рисунок 3 – Алгоритм обнаружения КА

1) Модуль «Захват и буферизация» выполняет захват и буферизацию трафика.

2) Захваченные данные трафика передаются в модуль «Сигнатурный анализ», который выявляет КА.

3) Захваченные данные трафика передаются в модуль «Эвристический анализ», который выполняет выявление КА.

4) В случае обнаружения КА сырые данные СИБ попадают в модуль «Обогащение СИБ». Модуль буферизирует поступающие сырые данные СИБ и обогащает данными о решающих правилах сигнатурного анализа, данными чёрных списков, справочными данными, информацией о хостах, данными географического местоположения. СИБ связывается с базой уязвимостей, рассчитывается индикатора достоверности угрозы.

5) СИБ после обогащения сохраняется в БД ПС Сенсор. Хранение СИБ обеспечивает модуль «Хранение больших данных».

6) Модуль «Уведомления» информирует пользователей ПК СОВ о появлении СИБ.

7) В случае обнаружения КА модуль «Копирование пакетов», используя захваченные пакеты, формирует PCAP-файл для созданного СИБ. В качестве имени PCAP-файла используется идентификатор СИБ.

8) PCAP-файл сохраняется. Хранение PCAP-файла обеспечивает модуль «Хранение файлов».

3.5.2 Алгоритм обучения

Блок-схема алгоритма обучения ПС Сенсор представлена на рисунке 4.

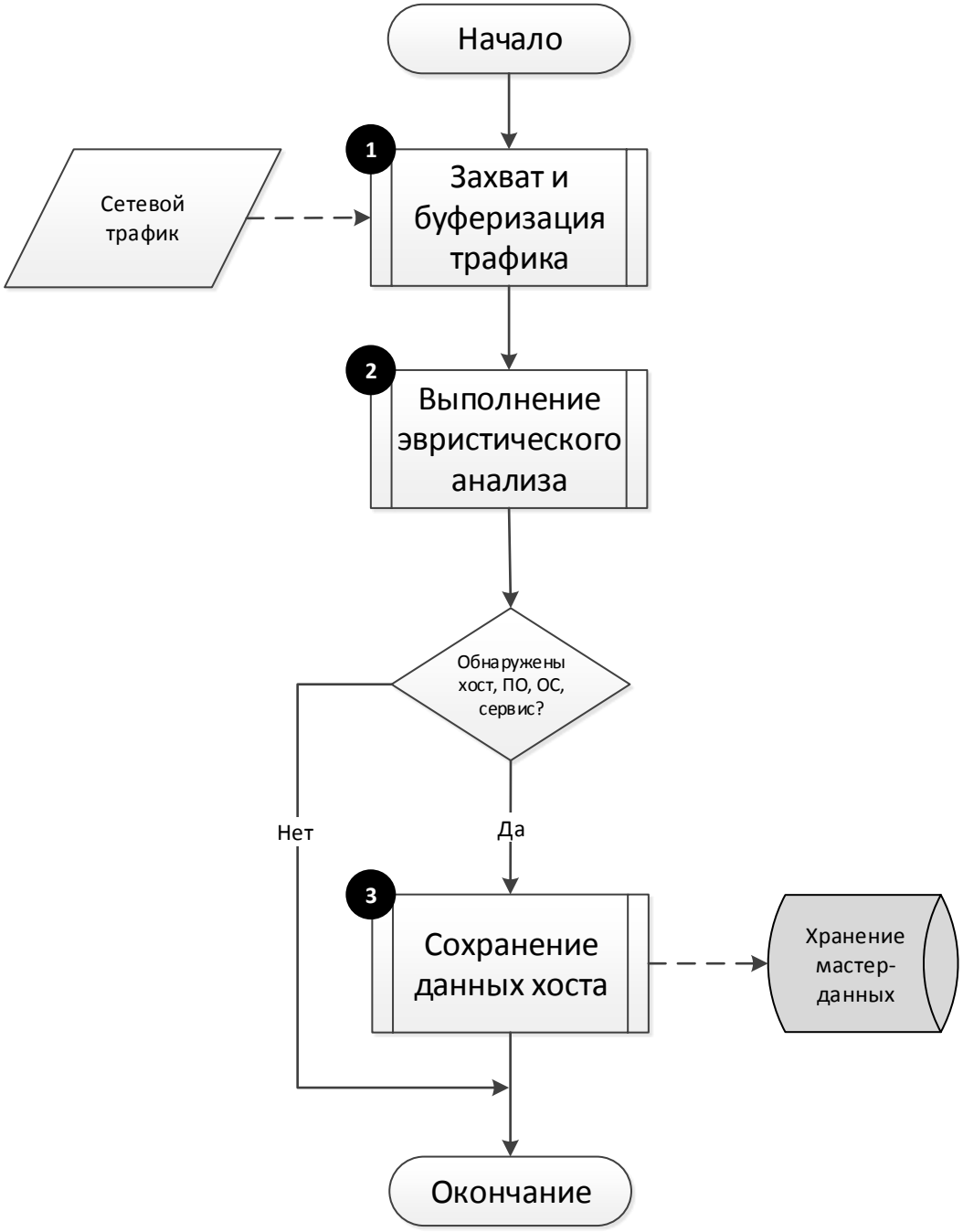

Рисунок 4 – Алгоритм обучения

1) Модуль «Захват и буферизация» выполняет захват и буферизацию трафика.

2) Захваченные данные трафика передаются в модуль «Эвристический анализ», который выполняет поиск новых хостов и программного обеспечения на них.

3) Информация об обнаруженных хостах, программных клиентах, сервисах, операционных системах сохраняется в БД ПС Сенсор, таким образом формируются профили хостов. Хранение профилей хостов обеспечивает модуль «Хранение мастер-данных».

В начале обучения, по его окончании и в случае возникновения ошибок обучения формируются события обучения в модуле «Аудит безопасности».

3.5.3 Алгоритм сбора статистики

Блок-схема алгоритма сбора статистики представлена на рисунке 5.

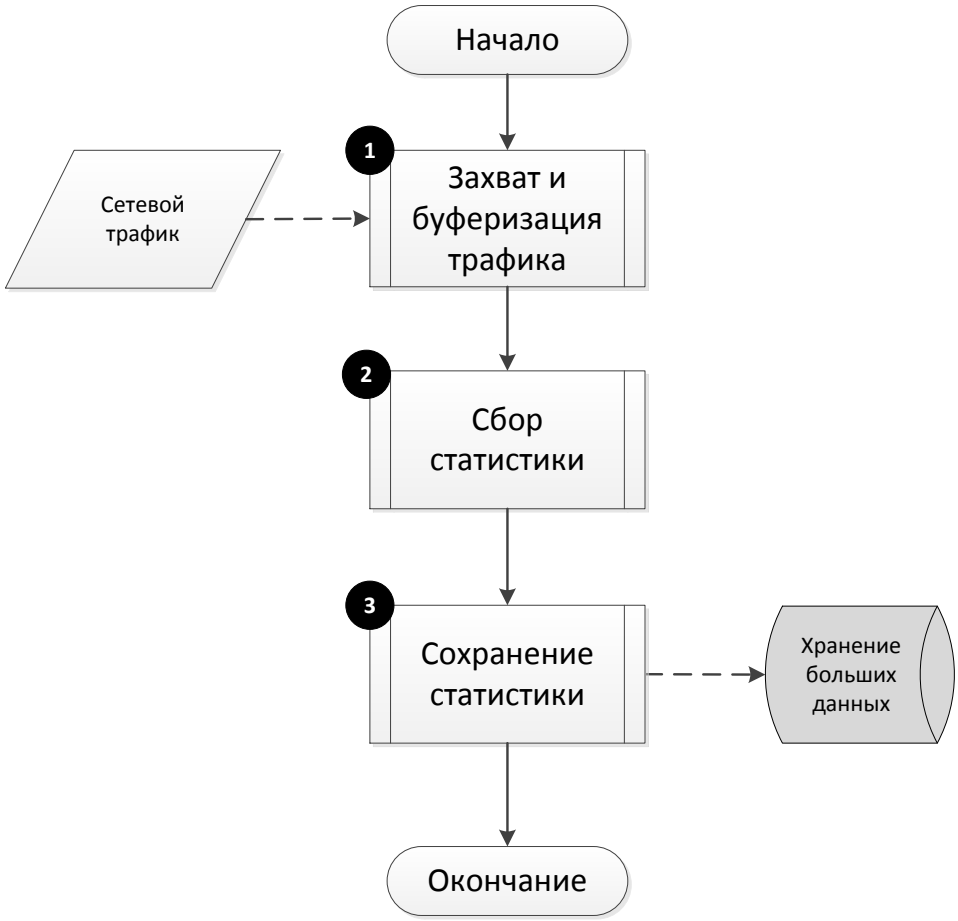

Рисунок 5 – Алгоритм сбора статистики

1) Модуль «Захват и буферизация» выполняет захват и буферизацию трафика.

2) Захваченные данные трафика передаются в модуль «Сбор статистики», который собирает статистику сетевого трафика.

3) Собранные статистические данные сохраняются в БД ПС Сенсор. Хранение обеспечивает модуль «Хранение больших данных».

В начале сбора статистики, по его окончании и в случае возникновения ошибок сбора статистики формируются события статистики в модуле «Аудит безопасности».

3.5.4 Алгоритм аудита безопасности

Блок-схема алгоритма аудита безопасности представлена на рисунке 6.

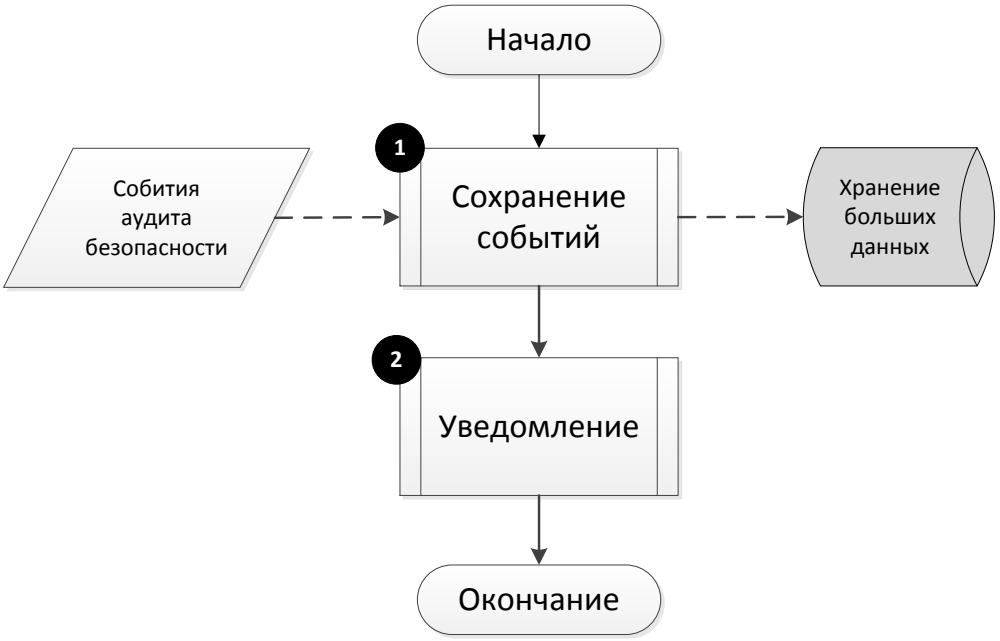

Рисунок 6 – Алгоритм аудита безопасности

1) Модуль «Аудит безопасности» принимает, обрабатывает и сохраняет события аудита безопасности в БД ПС ПК СОВ. Хранение обеспечивает модуль «Хранение больших данных».

2) Модуль «Уведомления» информирует пользователей ПК СОВ о возникших событиях аудита безопасности.

3.5.5 Алгоритм мониторинга состояния и работоспособности

Блок-схема алгоритма мониторинга состояния и работоспособности ПС ПК СОВ представлена на рисунке 7.

Рисунок 7 – Алгоритм мониторинга состояния и работоспособности

1) Модуль «Мониторинг состояний» принимает, обрабатывает и сохраняет показатели состояния и работоспособности ПС ПК СОВ в БД ПС ПК СОВ. Хранение показателей обеспечивает модуль «Хранение мастер-данных».

2) В случае превышения показателей пороговых значений модуль «Мониторинг состояний» передаёт событие мониторинга в модуль «Аудит безопасности».

3) Модуль «Передача и приём данных и команд» на периодической основе через заданные интервалы времени передаёт состояние ПС ПК СОВ в вышестоящий компонент.

3.5.6 Алгоритм выполнения команд

Блок-схема алгоритма выполнения команд представлена на рисунке 8.

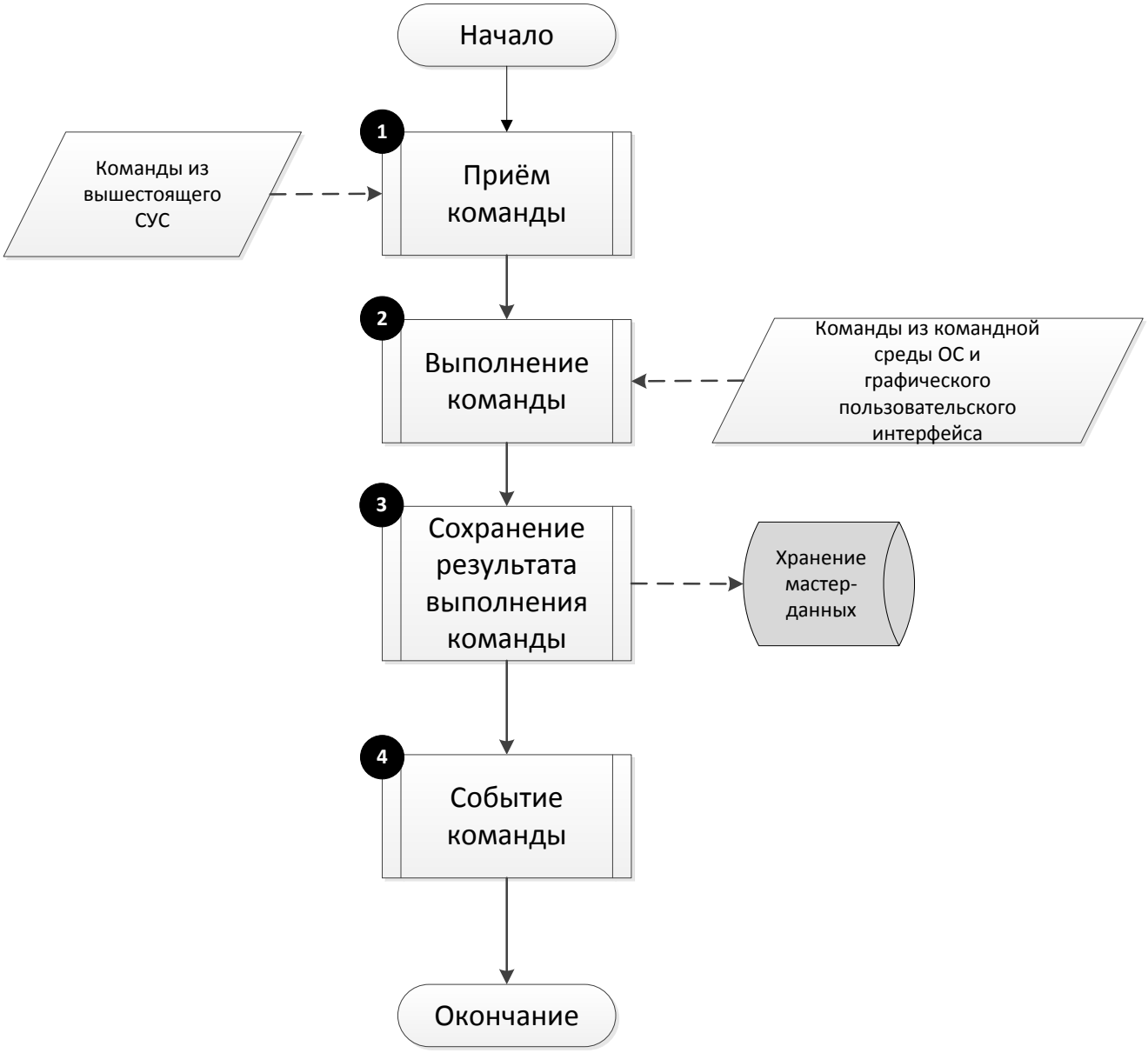

Рисунок 8 – Алгоритм выполнения команд

1) Поступающие из вышестоящего ПС СУС команды передаются в модуль «Выполнение команд». Передачу команд обеспечивает модуль «Передача и приём данных и команд».

2) Модуль «Выполнение команд» выполняет команды, поступающие из вышестоящего ПС СУС, из командной среды ОС, из модуля «Графический пользовательский интерфейс».

3) Результаты выполнения команд сохраняются в БД ПС СУС. Хранение результатов обеспечивает модуль «Хранение мастер-данных».

4) Модуль «Выполнение команд» передаёт событие команды в модуль «Аудит безопасности».

3.5.7 Алгоритм автоматического обновления БКЦ

Блок-схема алгоритма обновления БКЦ представлена на рисунке 9.

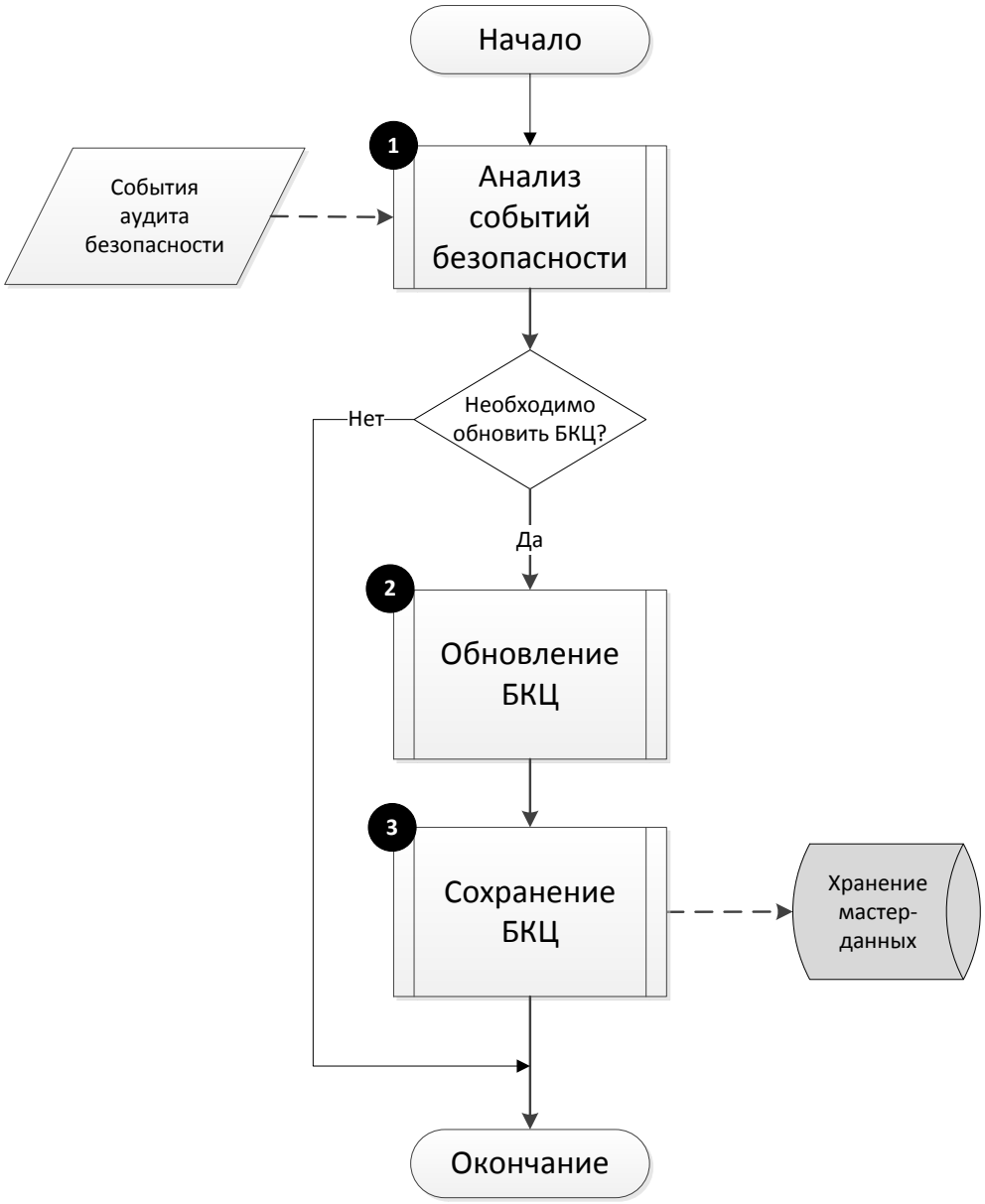

Рисунок 9 – Алгоритм автоматического обновления БКЦ

1) Модуль «Аудит безопасности» выполняет анализ событий аудита безопасности.

2) В случае появления событий аудита, связанных с обновлением ПС ПК СОВ, изменениями конфигурационных параметров настройки ПС ПК СОВ, модуль «Аудит безопасности» обновляет БКЦ в автоматическом режиме. Так же, в автоматическом режиме, БКЦ обновляется после завершения установки ПС Сенсор.

3) Обновлённая БКЦ сохраняется в БД ПС ПК СОВ. Хранение БКЦ обеспечивает модуль «Хранение файлов».

3.5.8 Алгоритм обновления (кроме справочных данных)

Блок-схема алгоритма обновления ПС ПК СОВ представлена на рисунке 10.

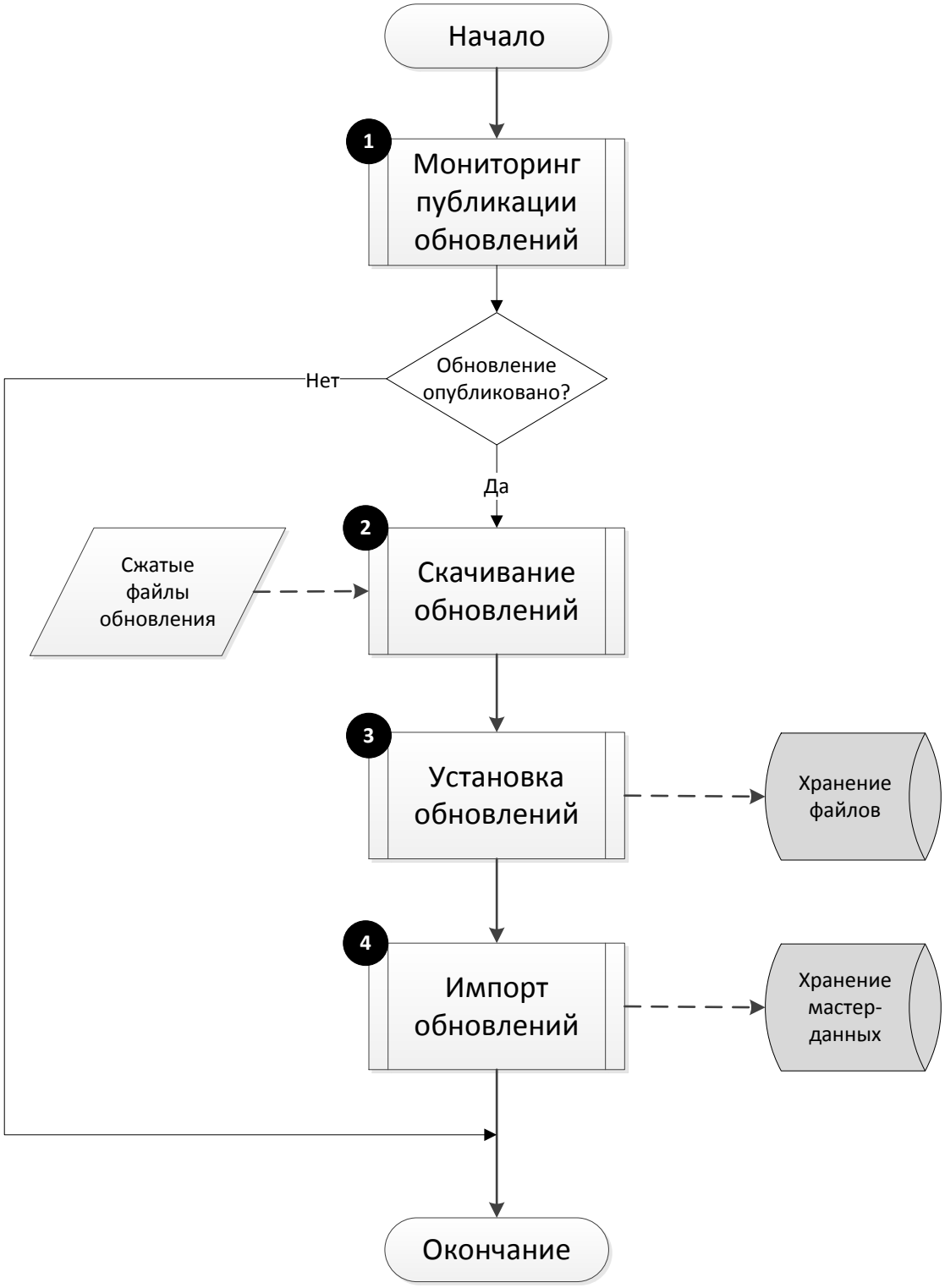

Рисунок 10 – Алгоритм обновления

1) Модуль «Обновление» запрашивает информацию о наличии обновлений.

Если СУС является корневым, на сервер обновления отсылается HTTP-запрос.

Если СУС не является корневым, то запрос уходит в вышестоящий СУС. Передачу запроса обеспечивает модуль «Передача и приём данных и команд».

2) При наличии обновлений модуль «Обновление» скачивает сжатые файлы обновлений.

Если СУС является корневым, то скачивание выполняется с помощью HTTPS-протокола.

Если СУС не является корневым, то скачивание выполняет модуль «Передача и приём данных и команд».

3) Модуль «Обновление» распаковывает файлы обновлений и выполняет следующие действия:

– размещает файлы сигнатур в модуле «Хранение файлов» (только для ПС Сенсор);

– размещает файлы чёрных списков в модуле «Хранение файлов» (только для ПС Сенсор);

– размещает файлы программных сценариев эвристического анализа в модуле «Хранение файлов» (только для ПС Сенсор);

– размещает базу GeoIP в модуле «Хранение файлов»;

– размещает данные картографии в модуле «Хранение файлов» (только для ПС СУС);

– обновляет ПО ПС ПК СОВ.

4) Модуль «Обновление» выполняет импорт данных обновлений в БД ПС Сенсор:

– базу решающих правил сигнатурного анализа;

– чёрные списки;

– справочники,

– базу уязвимостей.

Модуль «Обновление» регистрирует обновление в реестре обновлений.

Хранение импортированных данных и реестра обновлений обеспечивает модуль «Хранение мастер-данных».

В начале обновления, по окончании обновления и в случае возникновения ошибок обновления формируются события обновления в модуле «Аудит безопасности».

3.5.9 Алгоритм регистрации компонента

Блок-схема алгоритма регистрации компонента представлена на рисунке 11.

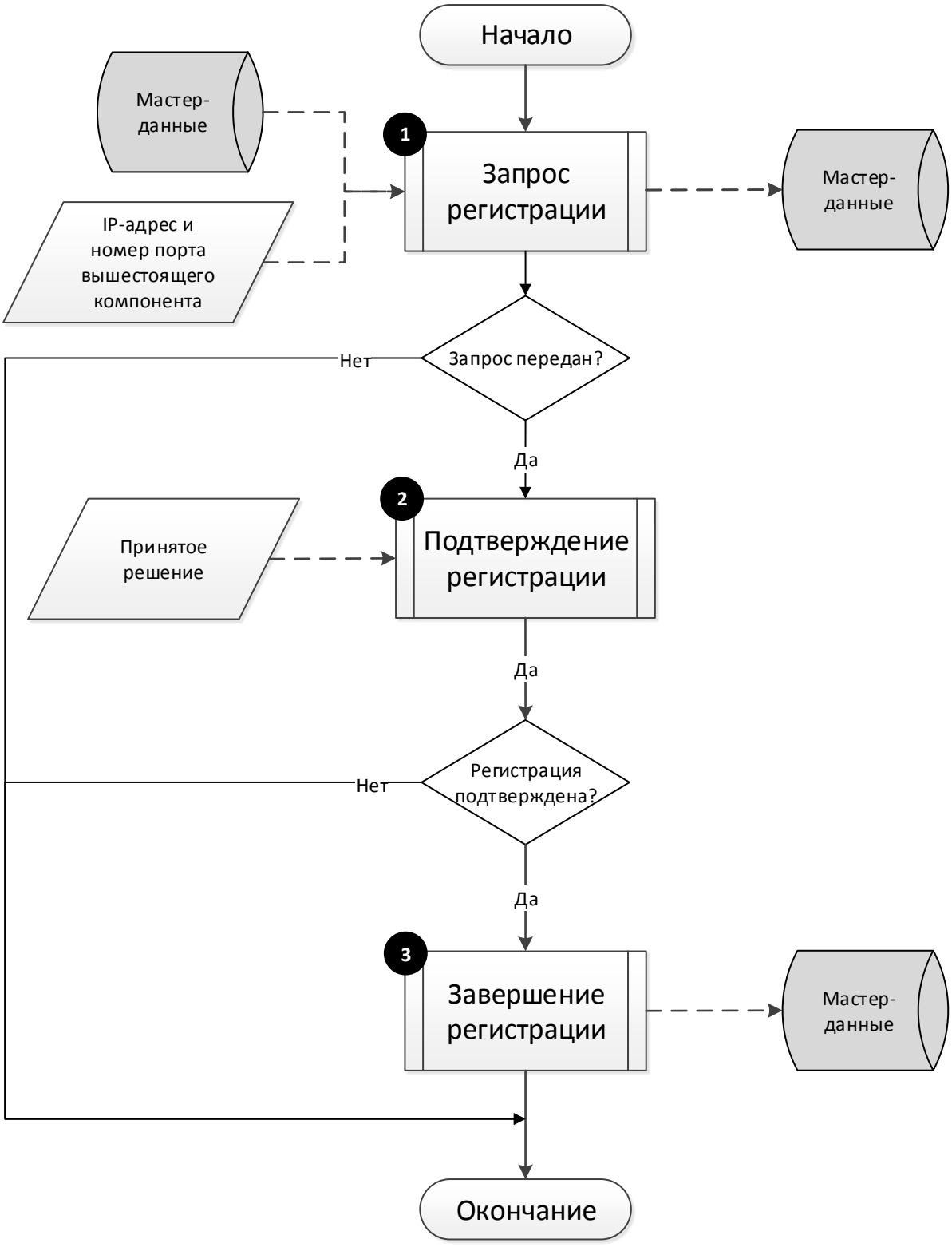

Рисунок 11 – Алгоритм регистрации компонента

1) Пользователь на регистрируемом компоненте инициирует запрос командой из командной среды ОС этого компонента. В команде указываются IP-адрес и номер порта вышестоящего компонента. Регистрируемый компонент формирует запрос регистрации, в который помещаются данные этого компонента, хранящиеся в модуле «Хранение мастер-данных». Запрос отправляется на вышестоящий компонент. Передачу запроса обеспечивает модуль «Передача и приём данных и команд». В вышестоящем компоненте запрос сохраняется в модуле «Хранение мастер-данных» в журнале регистрации компонентов.

2) Если на этапе запроса регистрации ошибки не возникли, то на вышестоящем компоненте пользователь принимает решение: подтвердить или отклонить запрос регистрации. Для этого используется модуль «Графический пользовательский интерфейс». На регистрируемый компонент отправляется ответ с принятым решением. Передачу обеспечивает модуль «Передача и приём данных и команд»

3) Если пользователь на этапе принятия решения подтвердил регистрацию, и во время передачи ответа ошибки не возникли, то:

– На вышестоящем компоненте в иерархии компонентов появляется подчинённый зарегистрированный компонент. Данные об иерархии компонентов хранятся в модуле «Хранение мастер-данных».

– На зарегистрированном компоненте в иерархии компонентов появляется вышестоящий компонент. Если зарегистрированный компонент является сенсором, то его статус меняется на «Не активный». Данные об иерархии компонентов и статусах компонентов хранятся в модуле «Хранение мастер-данных».

События, связанные с действиями в процессе регистрации и возникающими ошибками, фиксируются модулем «Аудит безопасности». Также проставляется отметка о результате регистрации в журнале регистрации обоих компонентов.

3.5.10 Алгоритм передачи данных

Модуль «Передача и приём данных и команд» обеспечивает передачу данных от ПС СУС в вышестоящий ПС СУС и в подчинённые компоненты.

3.5.11 Алгоритм регистрации на сервере обновлений

Блок-схема алгоритма регистрации ПС СУС на сервере обновлений представлена на рисунке 12.

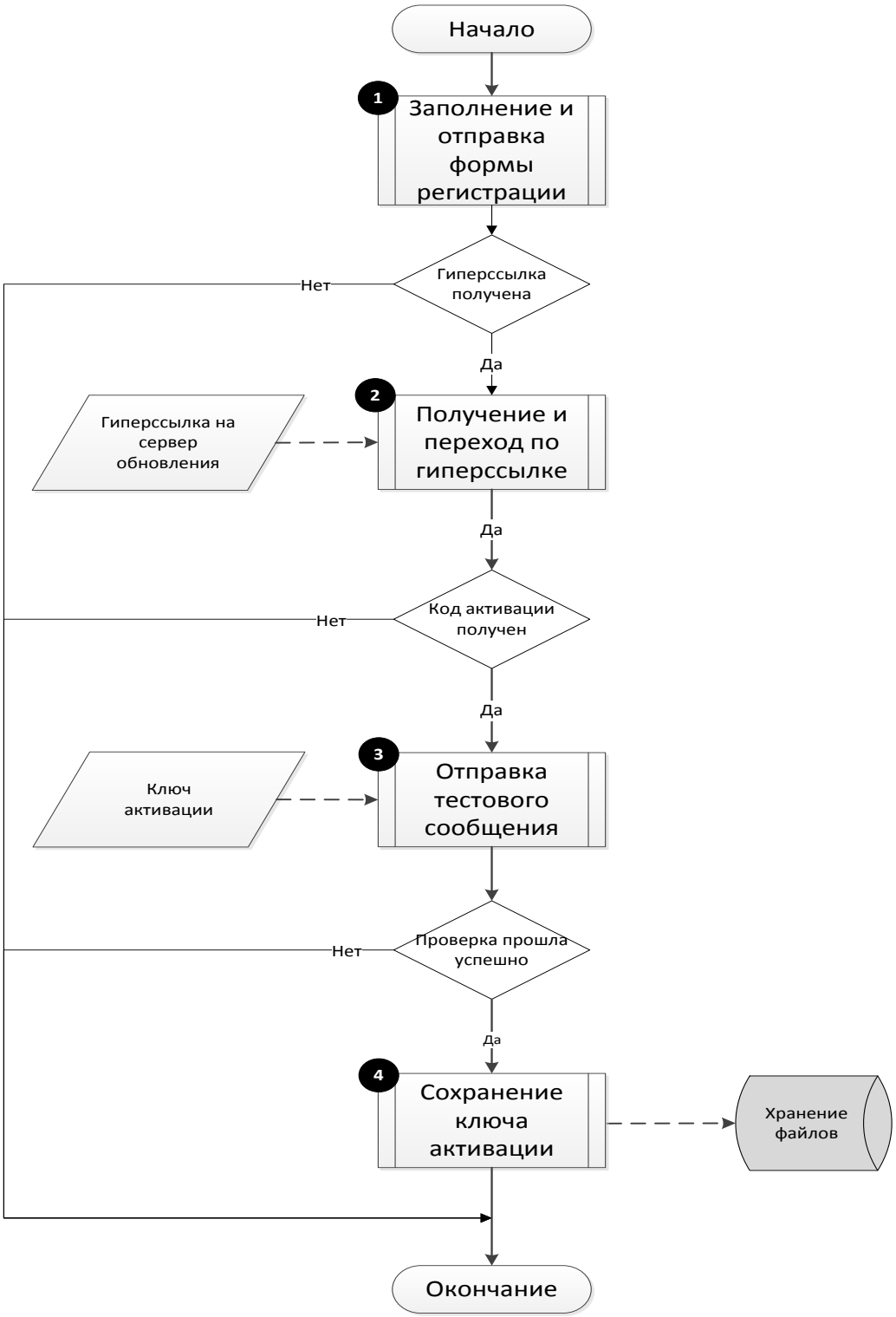

Рисунок 12 – Алгоритм регистрации на сервере обновлений

1) Пользователь ПС СУС с помощью модуля «Графический пользовательский интерфейс» заполняет форму регистрации и отправляет регистрационные данные на сервер обновления. Сервер обновления в ответ отправляет на электронный адрес пользователя гиперссылку на сервер обновления.

2) При поступлении электронного письма с сервера обновления пользователь ПС СУС переходит по гиперссылке. Сервер обновления отправляет на электронный адрес пользователя ключ активации для доступа к программному интерфейсу сервера обновления.

3) Пользователь переносит ключ активации в форму регистрации и завершает регистрацию, отправляя тестовое сообщение на сервер обновления. Сервер обновления проверяет тестовое сообщение и подтверждает активацию компонента ПК СОВ на сервере обновлений.

4) Ключ активации сохраняется в модуле «Хранение файлов».

3.5.12 Алгоритм смены статусов ПС Сенсор

ПС Сенсор может находиться в следующих статусах:

– Инициализация. Особенное состояние ПС Сенсор на время установки компонента.

– Не зарегистрирован. Состояние ПС Сенсор после установки компонента. Аналогично состоянию «Неактивный». До начала выполнения своих функций ПС Сенсор должно быть зарегистрировано.

– Неактивный. В жизненном цикле это состояние используется для временного отключения компонента, например, для перезагрузки оборудования, проведения регламентных работ. В этом состоянии в ПС Сенсор запущены следующие модули:

а) Выполнение команд,

б) Мониторинг состояний,

в) Передача и приём данных и команд.

– Обнаружение. Основное состояние ПС Сенсор, во время которого компонент выполняет функции СОВ. В этом состоянии в ПС Сенсор запущены все модули (см. раздел 3.3 Таблица 2). Модуль «Эвристический анализ» работает в режиме обнаружения.

– Обучение. В этом состоянии в ПС Сенсор запущены все модули (см. раздел 3.3 Таблица 2). Модуль «Эвристический анализ» одновременно работает в режиме обнаружения и обучения.

– Скомпрометирован. В это состояние объект переводится автоматически, если обнаружено нарушение целостности БКЦ. Нарушение целостности может привести к неопределённым статусам сервисов на ПС Сенсор. Необходимо провести проверку и, возможно, исправить или восстановить настройки ПС Сенсор. В этом состоянии в ПС Сенсор запущены все модули (см. раздел 3.3 Таблица 2). Модуль «Эвристический анализ» работает в режиме обнаружения. В этом состоянии Модуль «Обновление» не обновляет справочники «Пользователи» и «Роли пользователей».

Схема смены статусов ПС Сенсор представлена на а рисунке 13.

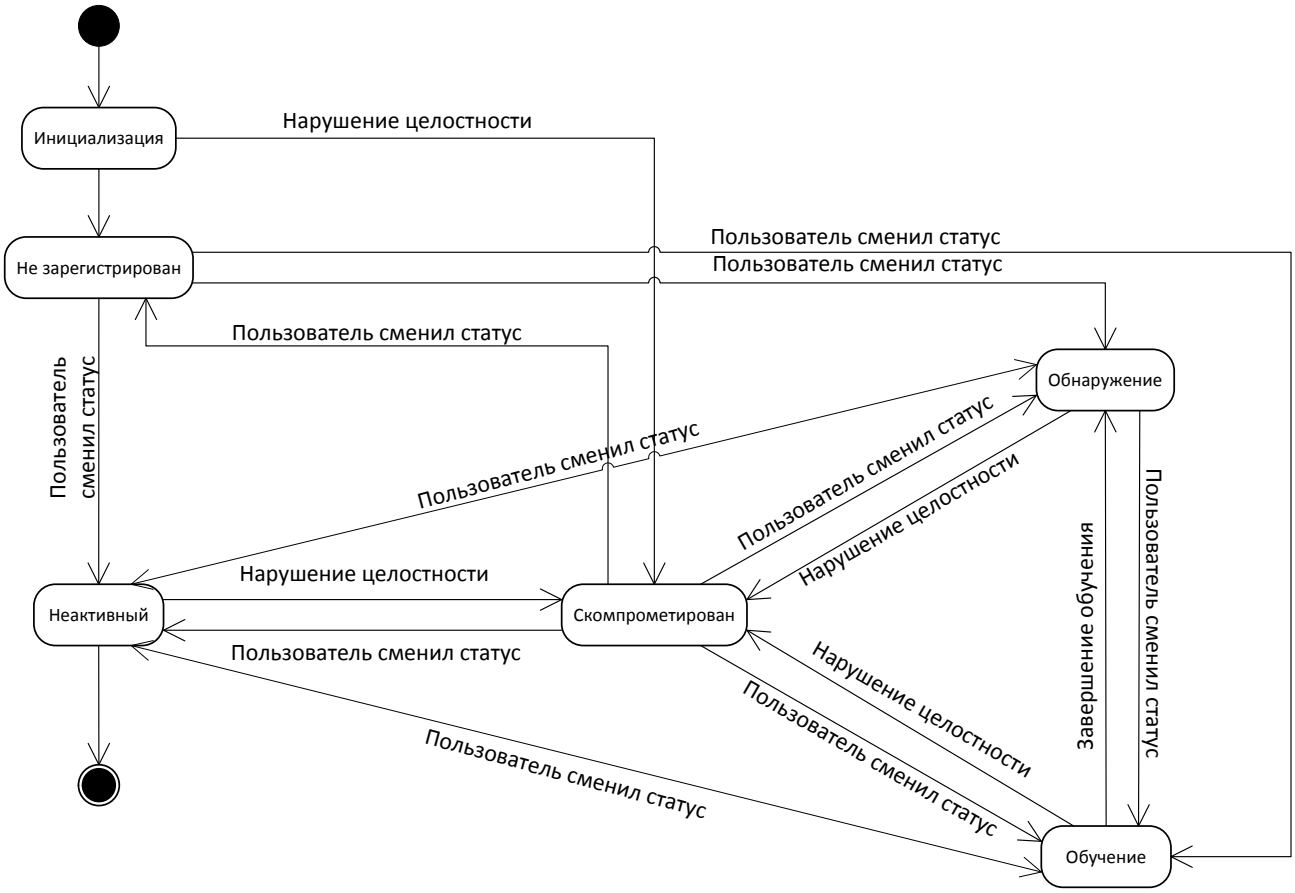

Рисунок 13 – Схема смены статусов ПС Сенсор

3.5.13 Алгоритм смены статусов ПС СУС

ПС СУС может находиться в следующих состояниях:

– Инициализация. Особенное состояние ПС СУС на время установки компонента.

– Неактивный. Начальное состояние ПС СУС после установки. В жизненном цикле это состояние используется для временного отключения компонента, например, для перезагрузки оборудования, проведения регламентных работ. В этом состоянии в ПС СУС запущены следующие модули:

а) Выполнение команд,

б) Мониторинг состояний,

в) Передача и приём данных и команд.

– Обнаружение. Основное состояние ПС СУС, во время которого компонент выполняет функции управления сенсорами. В этом состоянии в ПС СУС запущены все модули (см. раздел 3.3 Таблица 2).

– Скомпрометирован. В это состояние объект переводится автоматически, если обнаружено нарушение целостности БКЦ. Нарушение целостности может привести к неопределённым статусам сервисов на ПС СУС. Необходимо провести проверку и, возможно, исправить или восстановить настройки ПС СУС. В этом состоянии в ПС СУС запущены все модули (см. раздел 3.3 Таблица 2). В этом состоянии Модуль «Обновление» не выполняет обновление справочников «Пользователи» и «Роли пользователей».

На рисунке 14 представлена схема смены статусов ПС СУС.

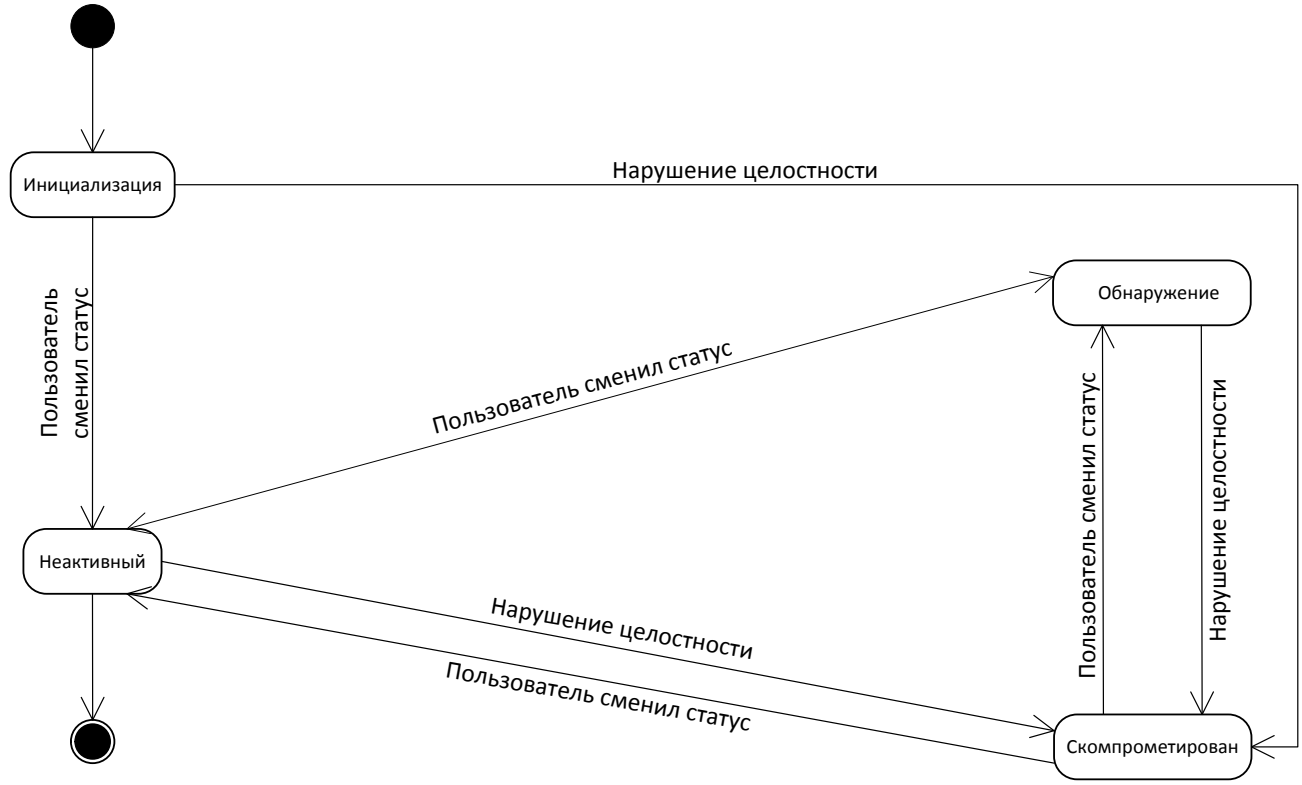

Рисунок 14 – Схема смены статусов ПС СУС

4 ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

ПК СОВ работоспособен на технических средствах под управлением ОС Astra Linux Special Edition «Смоленск» версии не ниже 1.5 с конфигурацией не хуже, чем указано в таблице 3.

Таблица 3 – Требования к техническим средствам

Наименование		**Требования к техническим средствам**	
		ПС Сенсор	**ПС СУС**
Процессор не хуже		Intel Core, не менее 2 ГГц	
Материнская плата не хуже		Совместимая с процессорами Intel Core	
Устройство хранения информации:	Интерфейс обмена данными, не хуже	SATA	
	Скорость вращения, не менее, rpm (об/мин)	7200	
	Форм-фактор, не менее	2,5	
	Объём памяти, не менее, Тбайт	1	2
	Контроллер RAID5/RAID10	Да	
Объём оперативной памяти, не менее, Гбайт		16	
Сетевое оборудование:	Сетевой интерфейс с поддержкой драйверов intel, не менее, 1 Гбит/с	Да	Да
	Сетевой интерфейс с поддержкой bypass, не менее, 1 Гбит/с	Да	Нет
	Qlogic Контроллер;	Нет	Да
Порт USB не хуже		USB 3.0.	
Консоль управления сервером iLOM с KVM и виртуальным CDROM		Да	

5 ВЫЗОВ И ЗАГРУЗКА

5.1 Вызов программы

Запуск ПС ПК СОВ выполняется автоматически:

- сразу после завершения инсталляции ПС ПК СОВ;
- после перезагрузки компонента с установленным ПС ПК СОВ.

Во время запуска выполняется старт сервисов – в соответствии со статусом компонента. После инсталляции ПС Сенсор находится в статусе «Не зарегистрирован», ПС СУС – в статусе «Не активный».

5.2 Входные точки в программу

Для того чтобы запустить графический пользовательский интерфейс, необходимо в командной строке веб-браузера ввести DNS-имя или IP-адрес компонента. Графический пользовательский интерфейс доступен только для ПС СУС.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	База данных
БКЦ	База контроля целостности
ГПИ	Графический пользовательский интерфейс
КА	Компьютерная атака
НЖМД	Накопитель на жёстких магнитных дисках
ПК	Программный комплекс
СОА	Система обнаружения атак
ОЗУ	Оперативное запоминающее устройство, оперативная память
ОС	Операционная система
ПО	Программное обеспечение
ПС	Программное средство
РПСА	Решающее правило сигнатурного анализа
СИБ	События информационной безопасности
СОА	Система обнаружения атак
СОВ	Система обнаружения вторжений
СУБД	Система управления базой данных
СУС	Сервер управления сенсорами
ЦПУ	Центральное процессорное устройство
ЭВМ	Электронная вычислительная машина
CLI	Comand line interface – интерфейс командной строки
MQTT	Message Queue Telemetry Transport –сетевой протокол, работающий поверх TCP/IP, применяемый для взаимодействия между устройствами (machine-to-machine)
SIEM	Security information and event management – класс ПО, который обеспечивает собор в одном месте событий, генерируемых различными системами информационной безопасности и корреляционный анализ событий в реальном времени

CEF	Common Event Format – формат данных, который применяется к данным, поступающим в SIEM-систему

ПЕРЕЧЕНЬ ТЕРМИНОВ

Администратор безопасности СОВ	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию СОВ
Браузер	Браузер – прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов . Также используется для управления веб-приложениями
Веб-приложение	Клиент-серверное приложение, в котором клиент взаимодействует с сервером при помощи браузера. В клиент-серверной архитектуре за работу сервера отвечает веб-сервер. Клиенты не зависят от конкретной операционной системы пользователя
Компонент	Сенсор – компонент регистрации событий. СУС – компонент анализа событий и управления сенсорами
Контролируемая система	Сегмент вычислительной сети, захват и анализ трафика которой выполняет сенсор
Корневой СУС	СУС, не имеющий вышестоящего СУС
Оператор визуального контроля СОВ	Уполномоченный пользователь, ответственный за анализ данных и формирование отчётов о СИБ, событиях аудита безопасности, статистике действий хостов контролируемой сети
Протокол	Стандарт передачи данных

Профиль хоста	Обобщённая информация о хосте, включающая в себя: – тип, имя, адрес, статус, важность, контролируемую систему; – показатели сетевой активности и статистику сетевого трафика; – установленные программные продукты и связанные с ними уязвимости; – перечень пользователей; – историю изменений
Сервер обновлений	Сервер – источник обновлений. Не является частью ПК СОВ
Сигнатура	Характерные признаки вторжения (атаки), используемые для его (её) обнаружения
Система обнаружения вторжения	Программное или программно-техническое средство, реализующее функции автоматизированного обнаружения (блокирования) действий в информационной системе, которые направлены на преднамеренный доступ к информации, или специальные воздействия на информацию (носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней
События СОА	Дополнительные данные, которые предоставляет СОА Bro в результате обработки сетевого трафика, позволяющие предоставить расширенную информацию для анализа СИБ. События СОА содержат данные о сетевых соединениях, сеансах протоколов прикладного уровня, уведомлениях о потенциально опасных событиях
Хост	Компьютер или сервер, подключённый к сегменту вычислительной сети контролируемой системы

Afick	Утилита аудита целостности, при котором выявляются несанкционированные изменения объектов ПК СОВ (ПО, конфигурационных файлов, базы решающих правил сигнатурного анализа, чёрных списков, программных сценариев эвристического анализа)
Bro	Сетевая система обнаружения вторжения. Является свободным программным обеспечением
C++	Компилируемый, статически типизированный язык программирования общего назначения
DNS-имя	Имя в системе доменных имён
ECMAScript	Встраиваемый, расширяемый, не имеющий средств ввода-вывода язык программирования, используемый в качестве основы для построения других скриптовых языков. Является расширением языка: JavaScript, JScript и ActionScript
GeoIP	База данных географического местоположения IP-адресов
HTTP-запрос	HTTP (HyperText Transfer Protocol) – протокол прикладного уровня передачи данных по технологии «клиент-сервер». Клиент инициирует соединение и посылает запрос серверу
HTTPS	HTTPS (HyperText Transfer Protocol Secure) – расширение протокола HTTP , поддерживающее защищенное соединение
IP-адрес	Уникальный сетевой адрес хоста в компьютерной сети, построенной на основе стека протоколов TCP/IP
MapServer	Серверная геоинформационная система
MD5-хеш	«Отпечаток» сообщения произвольной длины, созданный с помощью 128-битного алгоритма хеширования. Применяется для проверки целостности информации информации и хранения хешей паролей
Mosquitto MQTT broker	Брокер сообщений, который реализует протокол MQTT версии и обеспечивает выполнения обмена сообщениями с использованием модели публикации/подписки

Net-SNMP	Программное обеспечение, содержащее общие клиентские библиотеки, набор консольных приложений, расширяемый SNMP-агент для использования протокола SNMP. В задачи Net-SNMP входит управление сетевыми устройствами и получение информации об их работе, в частности о состоянии устройства: счетчики производительности, активные процессы, значения сетевого трафика на интерфейсах и т. д.
p0f	Утилита пассивного определения версии операционной системы на удаленном хосте с использованием метода сигнатурного анализа
Python	Высокоуровневый язык программирования общего назначения
SpatialDB	База пространственных данных
Suricata	Сетевая система обнаружения и предотвращения вторжения. Является свободным программным обеспечением
URL-адрес	Запись адреса, который указывает на расположение ресурса в интернете
Zabbix	Система мониторинга и отслеживания состояний сервисов компьютерной сети, серверов и сетевого оборудования

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	Номер документа	Входящий номер сопроводительного документа	Подпись	Дата
	изме-ненных	заменен-ных	новых	аннулиро-ванных					