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 73

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

Москва
2018

СОДЕРЖАНИЕ

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 Программное обеспечение, необходимое для функционирования программы

1.2.1 Программное обеспечение ПС Сенсор

1) ПС Сенсор функционирует под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2) ПС Сенсор для обнаружения сетевых вторжений в контролируемом канале передачи данных сигнатурным методом использует:

- Систему обнаружения атак (СОА) Suricata версии 4.0;
- СОА Bro версии 2.5.2;
- утилиту p0f версии 3.09b.

3) ПС Сенсор использует СОА Bro версии 2.5.2 для обнаружения сетевых вторжений в контролируемом канале передачи данных эвристическим методом обнаружения.

4) ПС Сенсор использует СУБД ClickHouse версии 1.1.54318 для хранения больших данных о событиях информационной безопасности (далее – СИБ), о журналах событий СОА, о событиях аудита безопасности и статистических данных сетевого трафика.

5) ПС Сенсор использует СУБД PostgreSQL версии 9.4 для хранения данных об объектах контролируемой системы, справочных данных, решающих правил сигнатурного анализа (РПСА), чёрных списков, базы уязвимостей.

6) ПС Сенсор использует программу-агент Net-SNMP версии 5.4.3 для мониторинга состояния и работоспособности. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix версии 2.2.7, входящее в состав поставки ПК СОВ.

7) ПС Сенсор использует утилиту Afick версии 2.1.3.21.3 для аудита целостности, при котором выявляются несанкционированные изменения объектов ПС Сенсор (ПО, конфигурационных файлов, базы решающих правил сигнатурного анализа, чёрных списков, программных сценариев эвристического анализа).

8) ПС Сенсор использует Mosquitto MQTT broker версии 3.1.1/3.1 для передачи данных и команд между ПС Сенсор и ПС СУС.

1.2.2 Программное обеспечение ПС СУС

1) ПС СУС функционирует под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2) ПС СУС использует СУБД ClickHouse версии 1.1.54327 для хранения больших данных о событиях информационной безопасности, журналах событий СОА, событиях аудита безопасности и статистических данных сетевого трафика.

3) ПС СУС использует СУБД PostgreSQL версии 9.4 для хранения данных об объектах контролируемой системы, справочных данных, решающих правил сигнатурного анализа, чёрных списков, базы уязвимостей.

4) ПС СУС использует программу-агент Net-SNMP версии 5.4.3 для мониторинга состояния и работоспособности ПС СУС. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix версии 2.2.7, входящее в состав поставки ПК СОВ.

5) ПС СУС использует утилиту Afick версии 2.1.3.21.3 для аудита целостности, при котором выявляются несанкционированные изменения объектов ПС СУС (ПО, конфигурационных файлов).

6) ПС СУС использует Mosquitto MQTT broker версии 3.1.1/3.1 для передачи данных и команд между ПС СУС и компонентами, расположенными ниже и выше по иерархии.

7) ПС СУС использует браузер, для выполнения функций ПС СУС, представленных в графическом пользовательском интерфейсе ПС СУС. ПС СУС совместимо со следующими браузерами: Firefox 44.0.2 из состава ОС Astra Linux Special «Смоленск».

1.2.3 Программные библиотеки, необходимые для функционирования ПК СОВ

Для функционирования ПК СОВ необходимы следующие программные библиотеки:

1) beaker версия 1.8.1;
2) clickhouse_driver версия 0.0.8;
3) configparser версия 3.5.0;
4) decorator версия 4.0.11;
5) falcon версия 1.2.0;
6) gostsum;
7) infi.clickhouse_orm версия 0.9.7.post5;
8) iniherit версия 0.3.6;
9) ipaddr версия 2.2.0;
10) jsonschema версия 2.6.0;
11) libc6 версия 2.4 и более поздние;
12) libgost;
13) libparsec-aud2;
14) libparsec-base2;
15) libpdp;
16) lockfile версия 0.12.2;
17) mod_wsgi версия 4.5.15;
18) msgpack_python версия 0.4.8;
19) numpy версия 1.12.1;
20) paho_mqtt версия 1.2.3;
21) pandas версия 0.19.2;

22) parsec-aud;

23) parsec-base;

24) parsec-mac;

25) peewee версия 2.10.1;

26) perl версия 5.14.2-21 и более поздние + deb7u2;

27) perlapi версия 5.14.2;

28) perl-tk;

29) pluton_yoyo версия 5.0.6.fix3.pluton;

30) psutil версия 5.2.2;

31) psycopg2 версия 2.7.1;

32) py_postgresql версия 1.2.1;

33) pygeoip версия 0.3.2;

34) pyinotify версия 0.9.6;

35) python_daemon версия 2.1.2;

36) python_dateutil версия 2.6.0;

37) python_mimeparse версия 1.6.0;

38) python_slugify версия 1.2.4;

39) python версия 3.5;

40) pytz версия 2017.2;

41) requests версия 2.14.2;

42) ruamel.yaml версия 0.15.9;

43) scipy версия 0.19.0;

44) six версия 1.10.0;

45) statsmodels версия 0.8.0;

46) texttable версия 0.8.8;

47) Unidecode версия 0.4.20;

48) valideer версия 0.4.2;

49) leaflet версия 1.2.0;

50) nDPI версия 2.0.0;

51) libhtp версии 0.5.23;

52) bro-af_packet-plugin;

53) qmqtt.

1.3 Языки программирования, на которых написана программа

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

1.4 Состав файлов, входящих в поставку программы

В поставку ПК СОВ входят, файлы, представленные в таблице 1.

Таблица 1 - Перечень файлов дистрибутива программы

Применяется для сенсора	**Применяется для СУС**	**Имя deb-файла**	**Описание**	**Контрольная сумма ГОСТ Р 34.11-2012**
Да	Да	pluton-audit_*_all.deb	Pluton Audit Service	83c762d513232ff797484b421605c92a6b05085d84c8a560dbe679087505c0e7
Да	Нет	pluton-bro-scripts_*_amd64.deb	Additional scripts for Bro	79cf31360358e1e77975ceffae01aad78b4241eb7646adcde5ec9c0df154f200
Да	Да	pluton-common-cpplib-dev_*_amd64.deb	Pluton Common library for C++ based libraries/services	300cb130ac11a86f4a54ba1ba550853608ee7ceb7a7fdaae77f726f3859e8229
Да	Да	pluton-common-py_*_all.deb	Pluton Common library for Python based libraries/services	3cbc3247549e2631025b769a0b57e9e2c4244ab92010a998bfc08557ebfff8a6
Да	Да	pluton-component-status_*_all.deb	Getting/updating component's status	bda3326a0a76d29eea0822510bdfe410c45a9e910294eb7246160ebe687b17d9
Да	Да	pluton-database_*_all.deb	Pluton database scripts. Contains tool for DB migration	ed2289dd6eba80c5859ed5962a8a79036bd7ad80b3c846d978a892a1cfa96b35
Да	Нет	pluton-event-logger_*_amd64.deb	Service for save bro events in Clickhouse	3f7a05335a3e9f564729f7b372e5a8ef88d27b6d5206a4ee23213fb9723b6cbb
Да	Нет	pluton-event-logger-watchdog_*_all.deb	Watchdog server for monitoring pluton-event-logger processes	dcd50d73c024b76d99cab32c5edd81ad9a53c92a0bc7c5844a780278f4fe57b1
Да	Да	pluton-health-monitor_*_all.deb	Daemon that reports system health stats using snmpd as a source	71ea32554243a3c8bcac2eed38f9282931576b09596fa36173427fed3f1dae17
Да	Нет	pluton-homenet-control_*_all.deb	Service and client for remote editing of HOME_NET for Bro and Suricata	27bc5ebffe53e93535ba82d8edfd7da7691f6b8d04a704a5fceafe889ecd9b71
Нет	Да	pluton-ise-handler_*_amd64.deb	Service for handling alerts	29a8f5a83aeb44f3e605473a7ba614818b242e291239a024a3cdcf670acf5b84
Да	Нет	pluton-ise-publisher_*_amd64.deb	Service for publishing alerts	3736a9f34aff7669c39333cfb6ecc137ef7d2cd74b2aabf8723d49156269dbb6

Применяется для сенсора	Применяется для СУС	Имя deb-файла	Описание	Контрольная сумма ГОСТ Р 34.11-2012
Да	Да	pluton-job-runner_*_all.deb	Daemon that starts various processes periodically using cron-like schedule stored in DB	884345467c98667e3e6117a02f6e356713576a395dce34e946aea5051afdfada
Да	Да	pluton-libisecache_*_amd64.deb	Library for saving alerts	8b357d6173ce954986b54d98fa2a41b9cf215913abc556483001c2301ede0dec
Да	Да	pluton-mqtt-transport-py_*_all.deb	Transport-layer service for MQTT-message exchange in component hierarchy.	56bfde238c2b7b32768b14a544840cd3dadde139882febef07cb0de683e30456
Да	Да	pluton-notification_*_all.deb	Pluton Notification Service	fa98076e9f1956576c046c69aed4a8cd8ae536c6ff262d3c76a1a1c877d651a5
Нет	Да	pluton-pcap-client_*_all.deb	Client API for pluton-pcap-server	e3ea87e44404219cc40f1a1b985ae302350fb92e001640b88d855dc8267667de
Да	Нет	pluton-pcap-generator_*_amd64.deb	Service for generating pcaps	7df0106ead93733e3e750edca0defd0b0582c0bacb77a387ef80567fb984dd43
Да	Нет	pluton-pcap-server_*_all.deb	Service for remote access to PCAP files	06ebc94c6f2cee117c13acc6bbcac46f24004a4ad98404cbde25bd49de87babf
Да	Нет	pluton-profile-generator_*_all.deb	Service for updating profiles and replication	8a91da113c97b6cd64f586fcd5780822eead79708ece8d45bae58adeccefb16d
Да	Да	pluton-query-service_*_all.deb	Client and daemon for sending queries to remote components	5e916e89e45f587c5ae15b317b2da8741b8c2bcf7f81cf240fe7b5c1dc018f4a
Да	Да	pluton-registration_*_all.deb	Pluton Component Registration Service	820383f058a1d3f0be6d8a5c9798adb0a9990460f2d0c99a68a68b6b3386c3d1
Да	Нет	pluton-rules-control_*_all.deb	Activation/deactivation of the signature rules	9c41d23bac35c16f600c7ab79b576b549e19ad653df8fd08dbe7267c035e5c5a
Нет	Да	pluton-scs-config_*_amd64.deb	no description given	c5eef76db8c52f8c76f8c868dfc2ef440ea809b7c9b530746a2e7e8ecf4840a8
Да	Нет	pluton-sensor-config_*_amd64.deb	no description given	553cc04cb316ccb4f69120f1179ee9c4c2bd18182b2ae818f11e50fa6a23ecc7
Да	Нет	pluton-stat-collector_*_amd64.deb	Service to collect network (nDPI) statistics into clickhouse db	bfe05187ebaba6713156d291957fb4a0bb0295b7075e0fdf4ffd608c1f80a30f
Да	Да	pluton-updater_*_all.deb	Pluton updater for different subsystems	c98b5bcddf70174856b11631a66c25184de19f91cb144c0ad3d81c01c7b2f1f2
Да	Да	pluton-user-control_*_all.deb	Pluton user control consol. Contains tool for user control	a47d5345406f735bcd47d1d413a4d82556e0485eff721745011956cc01efee0a
Нет	Да	pluton-web-backend_*_all.deb	Pluton SCS Web backend	b4b161bb28d014af0346136a113120c598a71c8c58cfa771c7187cd6ca7f29db

Применяется для сенсора	Применяется для СУС	Имя deb-файла	Описание	Контрольная сумма ГОСТ Р 34.11-2012
Нет	Да	pluton-web-frontend_*_amd64.deb	Pluton SCS Web Frontend	171be7a30c67c6fe454227a90f311bccfe66c260b94630c600f80975c9528a14

* - номер версии

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, событиях СОА;

– 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 AF_PACKET 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 СОА. Сигнатурный анализ реализуется с помощью СОА Suricata, СОА Bro и утилиты p0f.

Правила сигнатурного анализа хранятся в виде файлов. Хранение данных обеспечивает модуль «Хранение файлов». Местоположение файлов указано в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

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

Выходная информация: сырые данные СИБ.

Используемые сервисы:

– pluton-ise-publisher.

Используемые программные библиотеки:

– pluton-libisecache.

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.

Модуль использует СОА Bro. Программные сценарии эвристического анализа хранятся в виде файлов. Хранение данных обеспечивает модуль «Хранение файлов». Местоположение файлов указано в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

Входная информация: пакеты сетевого трафика.

Выходная информация: сырые данные СИБ, данные профилей хостов.

Используемые сервисы:

– pluton-ise-publisher;

– pluton-event-logger – сохраняет события СОА в модуле «Хранение больших данных».

Используемые программные библиотеки:

– libsensor-status.

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). Структура и атрибутивный состав данных статистики представлены в документе "ПК «СОВ «Плутон-М1.0».

Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

Входная информация: захваченные пакеты сетевого трафика.

Выходная информация: статистика, события статистики.

Используемые сервисы:

– pluton-stat-collector.

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.

Используемые сервисы:

– pluton-pcap-generator.

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.

---

1) PCAP-файл создаётся только для сигнатурных событий Suricata

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). Для аудита целостности применяется утилита Afick.

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.

Используемые сервисы:

– pluton-audit-server.

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.

Структура и атрибутивный состав данных, используемых для обогащения СИБ, представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. Местоположение файла базы GeoIP представлено в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81.

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

Выходная информация: СИБ.

Используемые сервисы:

– pluton-ise-publisher.

Используемые программные библиотеки:

– pluton-libisecache.

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.

– Модуль использует в своей работе программу-агент Net-SNMP для мониторинга состояния и работоспособности ПС СУС. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix, входящее в состав поставки ПК СОВ.

Показатели состояния и работоспособности сохраняются в БД ПС ПК СОВ. Для хранения используется модуль «Хранение мастер-данных» (см. раздел 3.2.12). Структура и атрибутивный состав данных состояний и работоспособности представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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.

Используемые сервисы:

– pluton-health-monitor.

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». Местоположения обновлённых файлов в файловой системе ОС указаны в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

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). Структура и атрибутивный состав импортируемых данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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. Структура и атрибутивный состав справочников представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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». Местоположения в файловой системе ОС обновлённых файлов указаны в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

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). Структура и атрибутивный состав импортируемых данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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». Местоположения в файловой системе обновлённых файлов указаны в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

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). Структура и атрибутивный состав импортируемых данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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. Структура и атрибутивный состав справочников представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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.

Используемые сервисы:

– pluton-updater-server.

Используемые команды:

– pluton-install-update – устанавливает обновление на компоненте.

3.2.11 Модуль «Хранение больших данных»

Модуль используется для хранения следующих видов данных:

– СИБ;

– журналы событий СОА;

– события аудита безопасности;

– статистика сетевого трафика.

Модуль использует для хранения СУБД ClickHouse, которая обладает необходимыми характеристиками производительности чтения и добавления больших данных. Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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 использует для хранения СУБД PostgreSQL, которая обладает необходимыми характеристиками для чтения, добавления, изменения, удаления данных с возможностью поддержки транзакционной целостности. Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

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.

Местоположение файлов указано в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

Модуль поддерживает функции:

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

– восстановление данных из резервной копии;

– архивирование;

– удаление исторических данных.

Используемые сервисы:

– pluton-pcap-generator – хранение PCAP-файлов;

– pluton-update-server – хранение файлов обновлений.

3.2.14 Модуль «Выполнение команд»

Модуль обеспечивает выполнение команд, которые инициируются:

– из командной среды ОС ПС ПК СОВ (см. перечень команд в документах "ПС «Сенсор-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.183-01 32 и "ПС «СУС-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.182-01 32);

– 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 2 представлен перечень команд:
Таблица 2 – 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	

Команда	ГПИ	Командная среда ОС
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.

Используемые сервисы:

– pluton-registration-server – регистрации компонентов;

– pluton-rules-control – активирование/деактивирование РПСА и чёрных списков;

– pluton-profile-generator – генерация профилей из данных СОА Bro;

– pluton-component-status-server – управление статусом компонентов.

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 СОА;
  - 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. Полное описание представлено в "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

Используемые сервисы:

- pluton-transport-server – доставка сообщений по иерархии компонентов;
- pluton-ise-publisher – передача СИБ из ПС Сенсор в ПС СУС;
- pluton-ise-handler – приём СИБ в ПС СУС;
- pluton-pcap-server – передача PCAP-файлов вверх по иерархии компонентов;
- pluton-updater-server – репликация данных по иерархии (кроме СИБ), установка обновлений;
- pluton-query-server – поддержка запросов в БД смежных компонентов.

Модуль использует программные библиотеки:

– pluton-libisecache.

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-component-status-server управляет статусами компонентов.

– Сервис pluton-event-logger-watchdog следить за работой сервисов ПК СОВ.

– 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.

Подробно о применении команд см. документы "ПС «Сенсор-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.183-01 32 и "ПС «СУС-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.182-01 32.

– 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 3 представлена информация о применении модулей ПК СОВ в ПС Сенсор и ПС СУС.

Таблица 3 – 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

Модуль	**ПС Сенсор**	**ПС СУС**
Передача и приём данных и команд	Да	Да

На рисунке 1 представлена логическая схема ПС Сенсор.

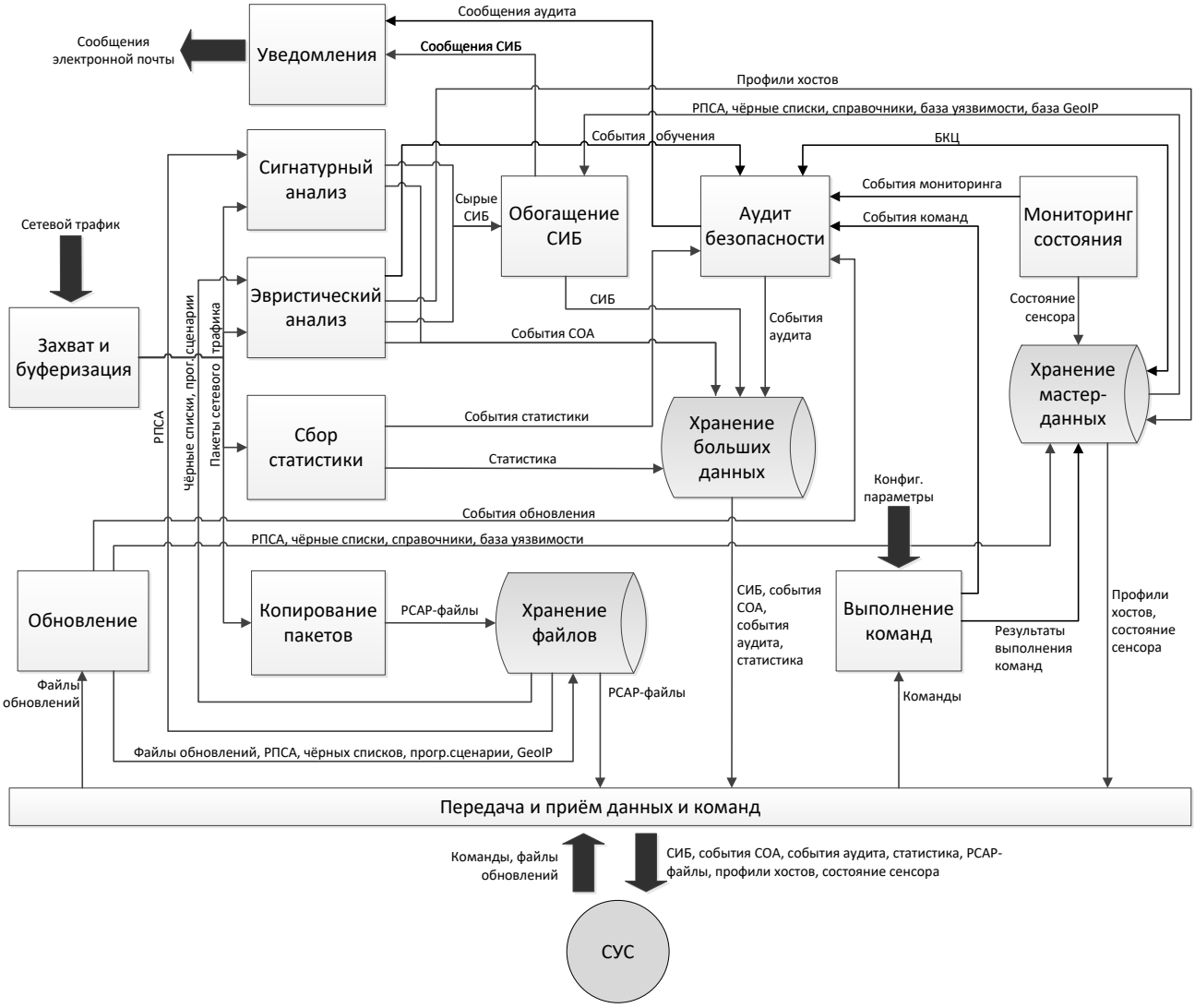

Рисунок 1 – Логическая схема ПС Сенсор

На рисунке 2 представлена логическая схема ПС СУС.

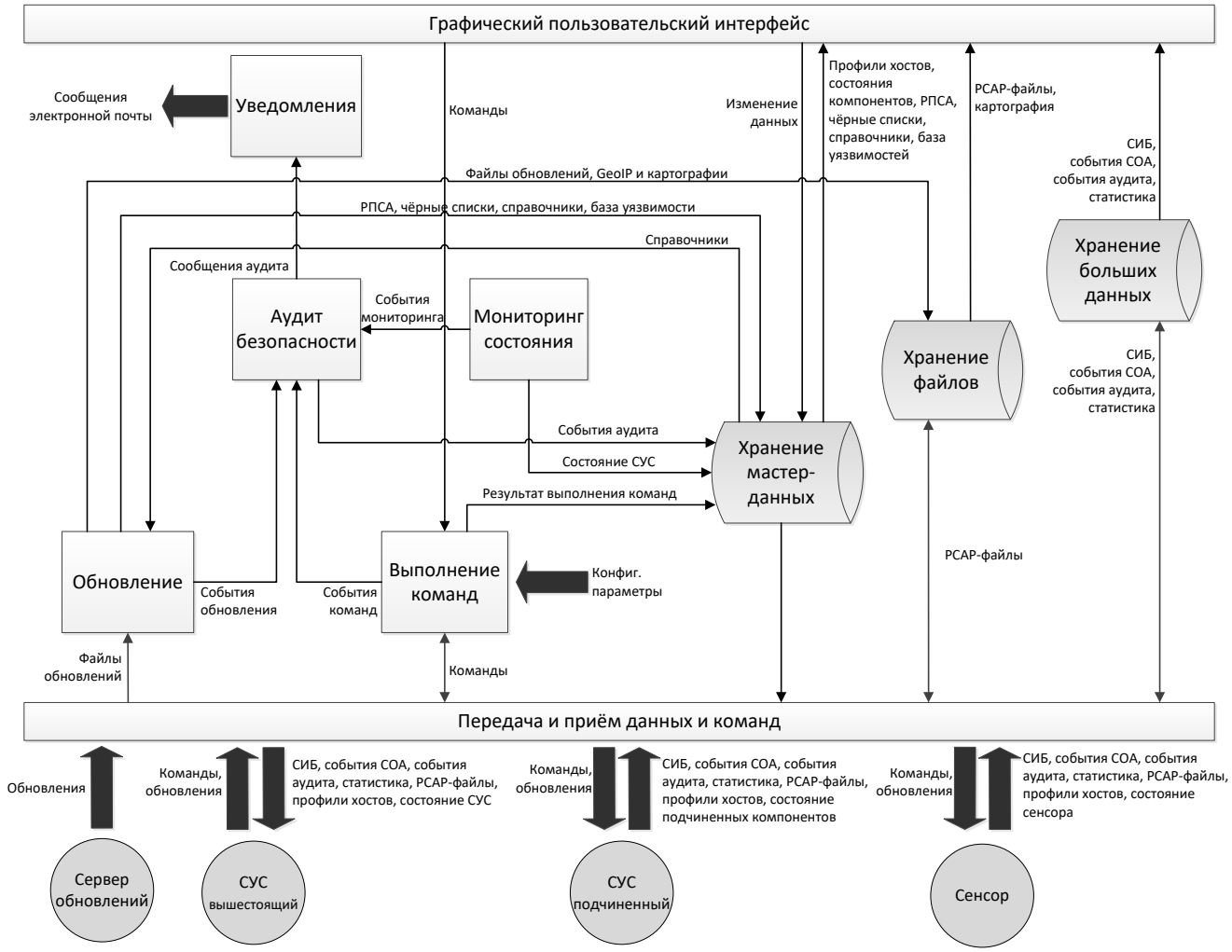

Рисунок 2 – Логическая схема ПС СУС

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.

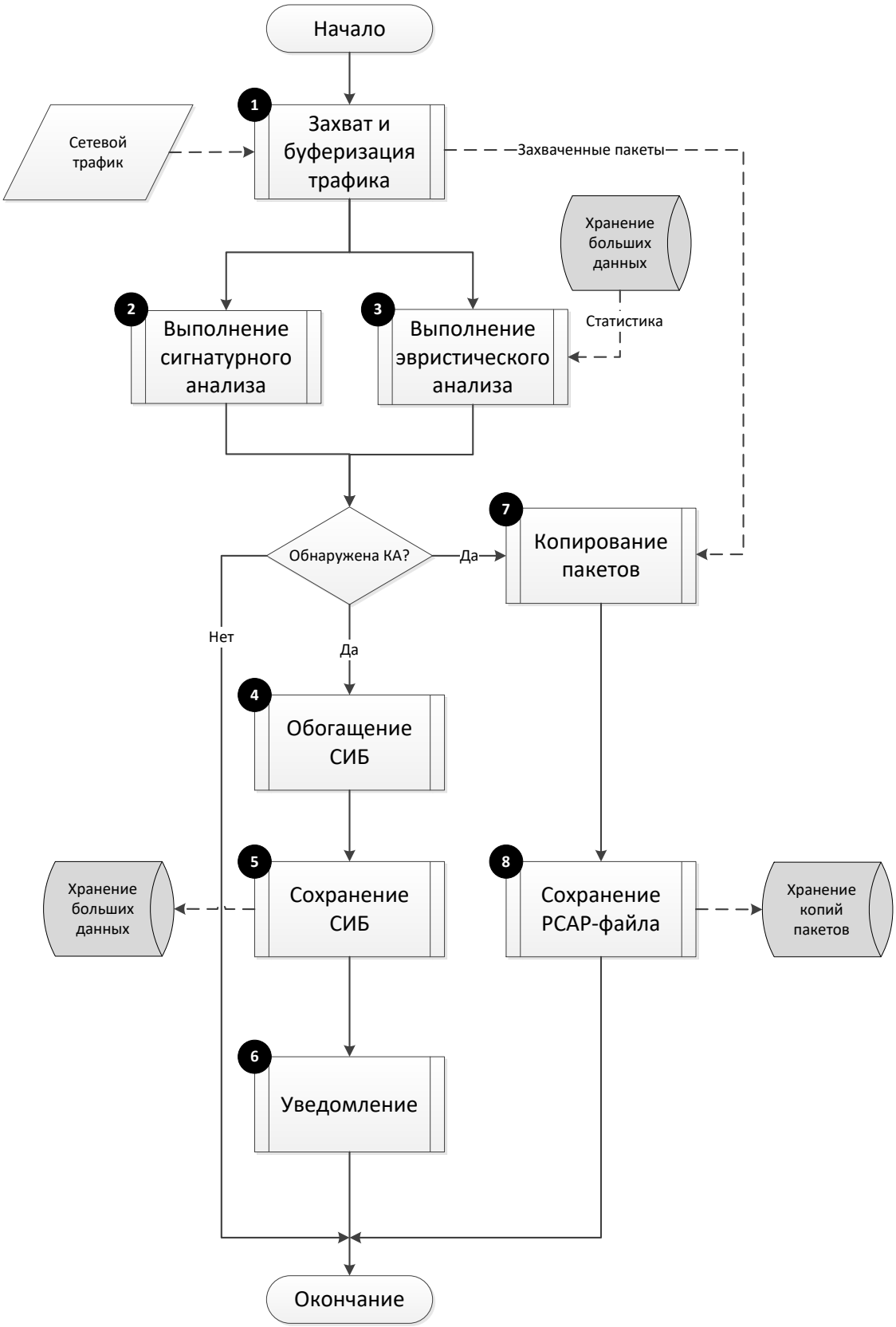

Рисунок 3 – Алгоритм обнаружения КА

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».

Структура и атрибутивный состав СИБ представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

3.5.2 Алгоритм обучения

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

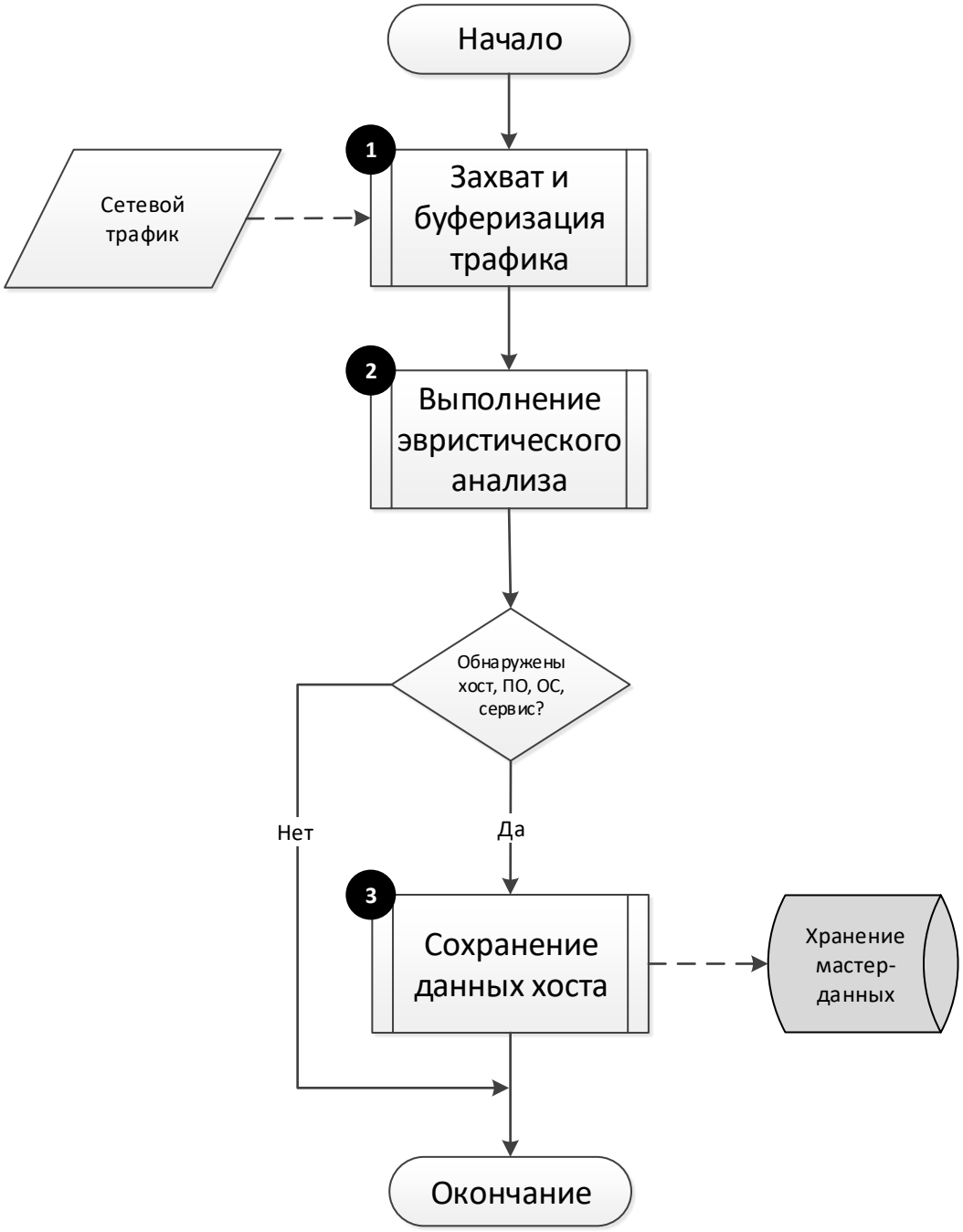

Рисунок 4 – Алгоритм обучения

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.

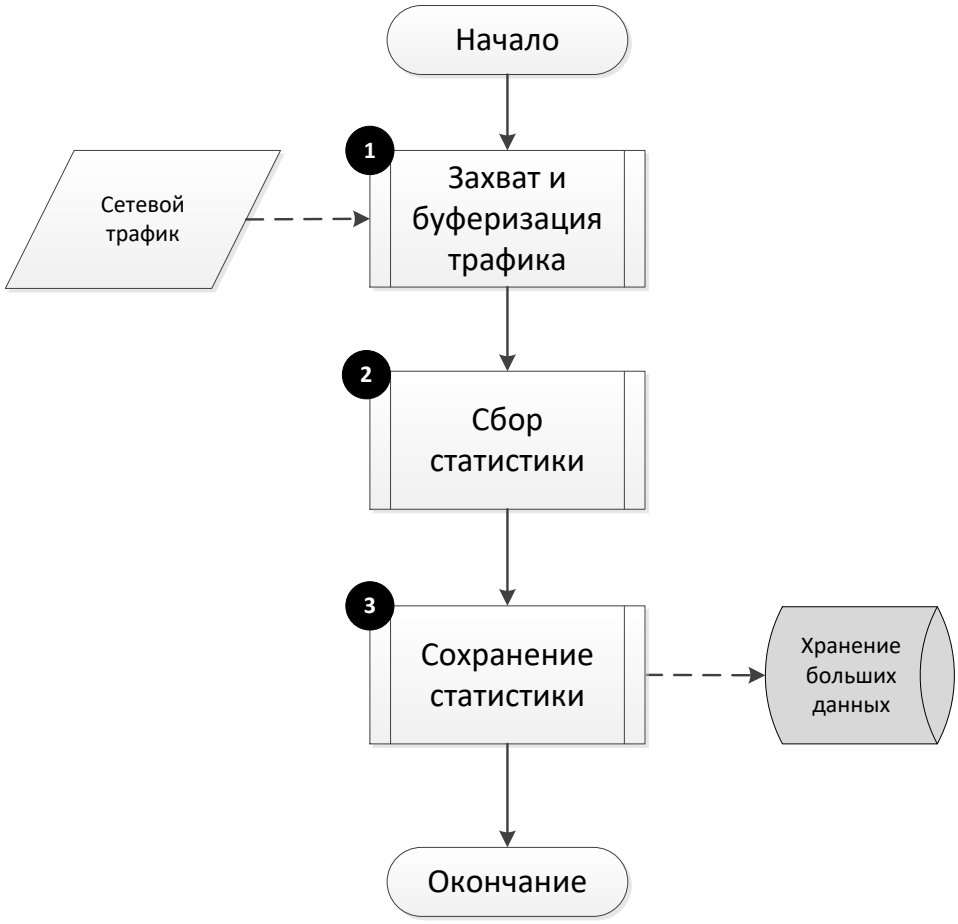

Рисунок 5 – Алгоритм сбора статистики

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.

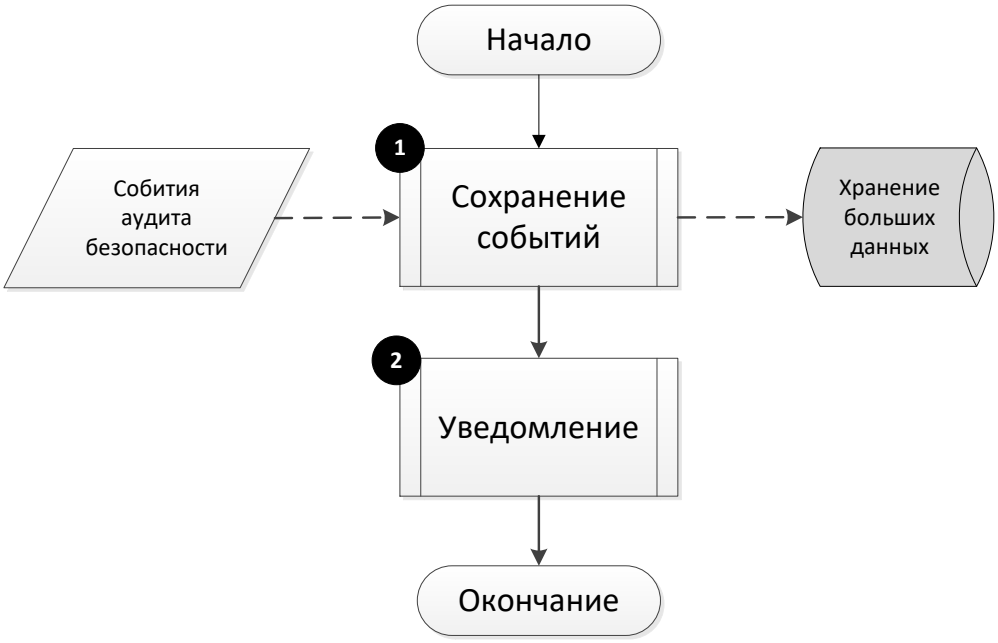

Рисунок 6 – Алгоритм аудита безопасности

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.

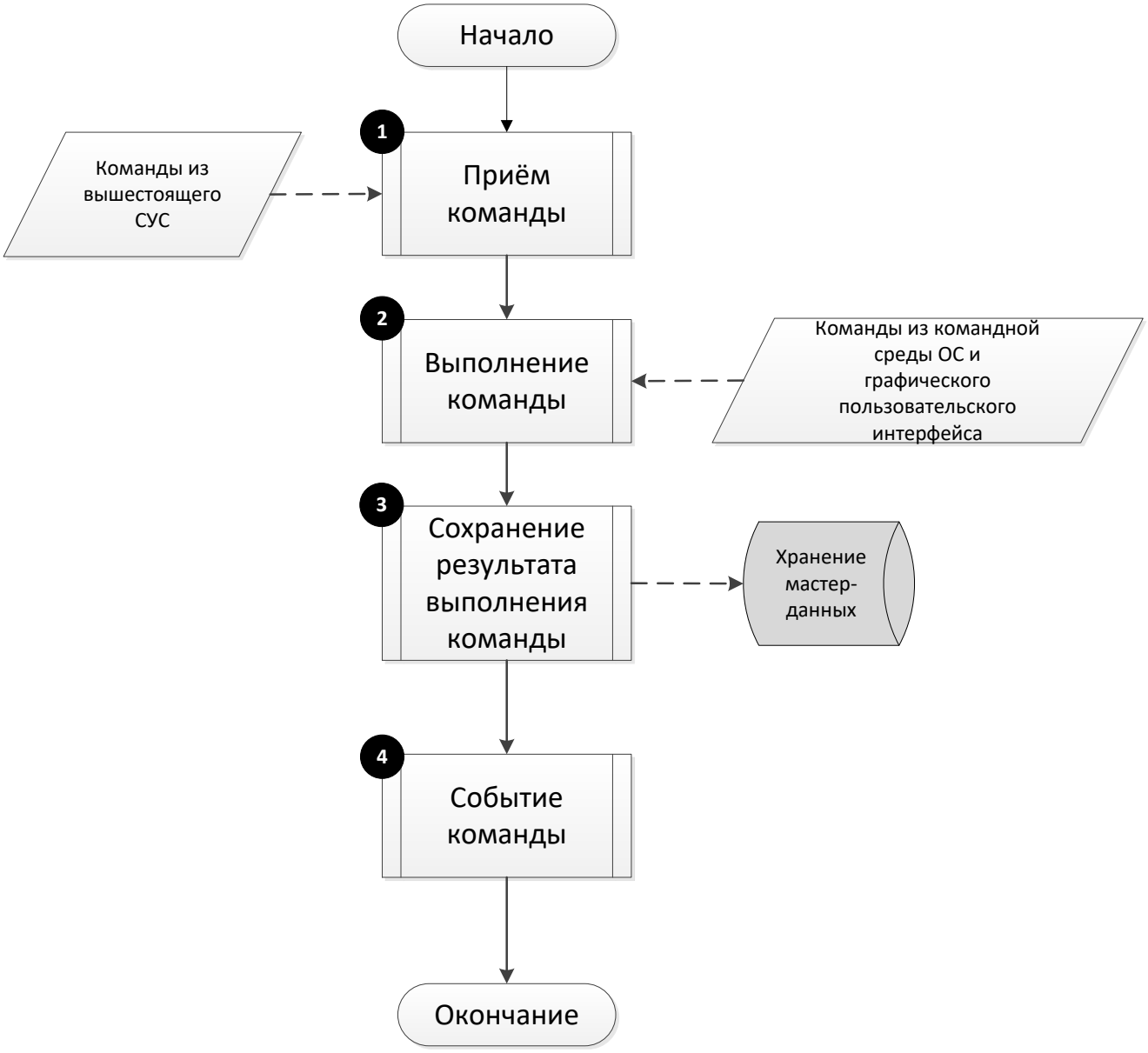

Рисунок 8 – Алгоритм выполнения команд

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».

Подробно алгоритмы и программный интерфейс взаимодействия компонентов ПК СОВ описаны в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

3.5.7 Алгоритм автоматического обновления БКЦ

Блок-схема алгоритма обновления БКЦ представлена на рисунке 9.

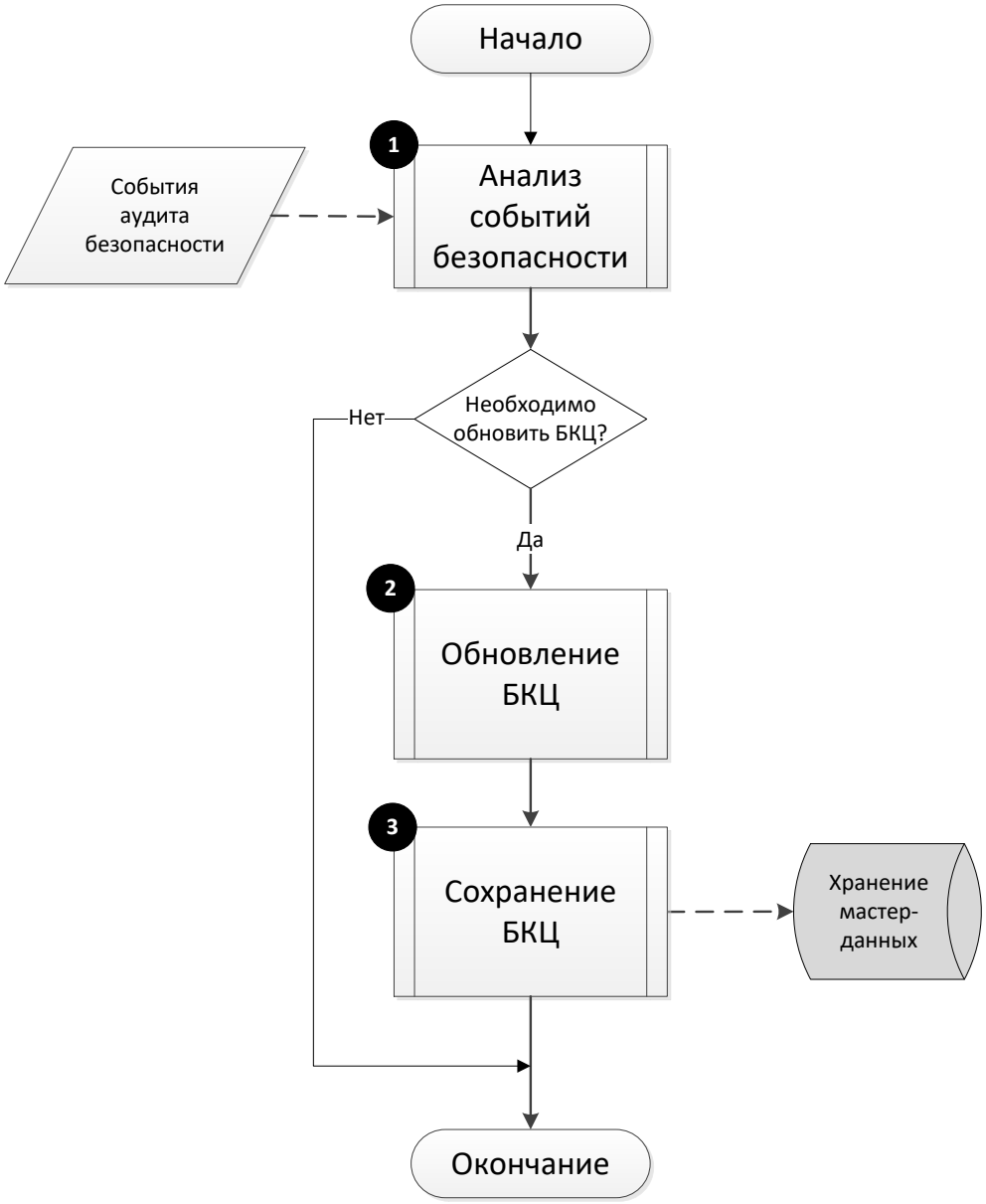

Рисунок 9 – Алгоритм автоматического обновления БКЦ

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.

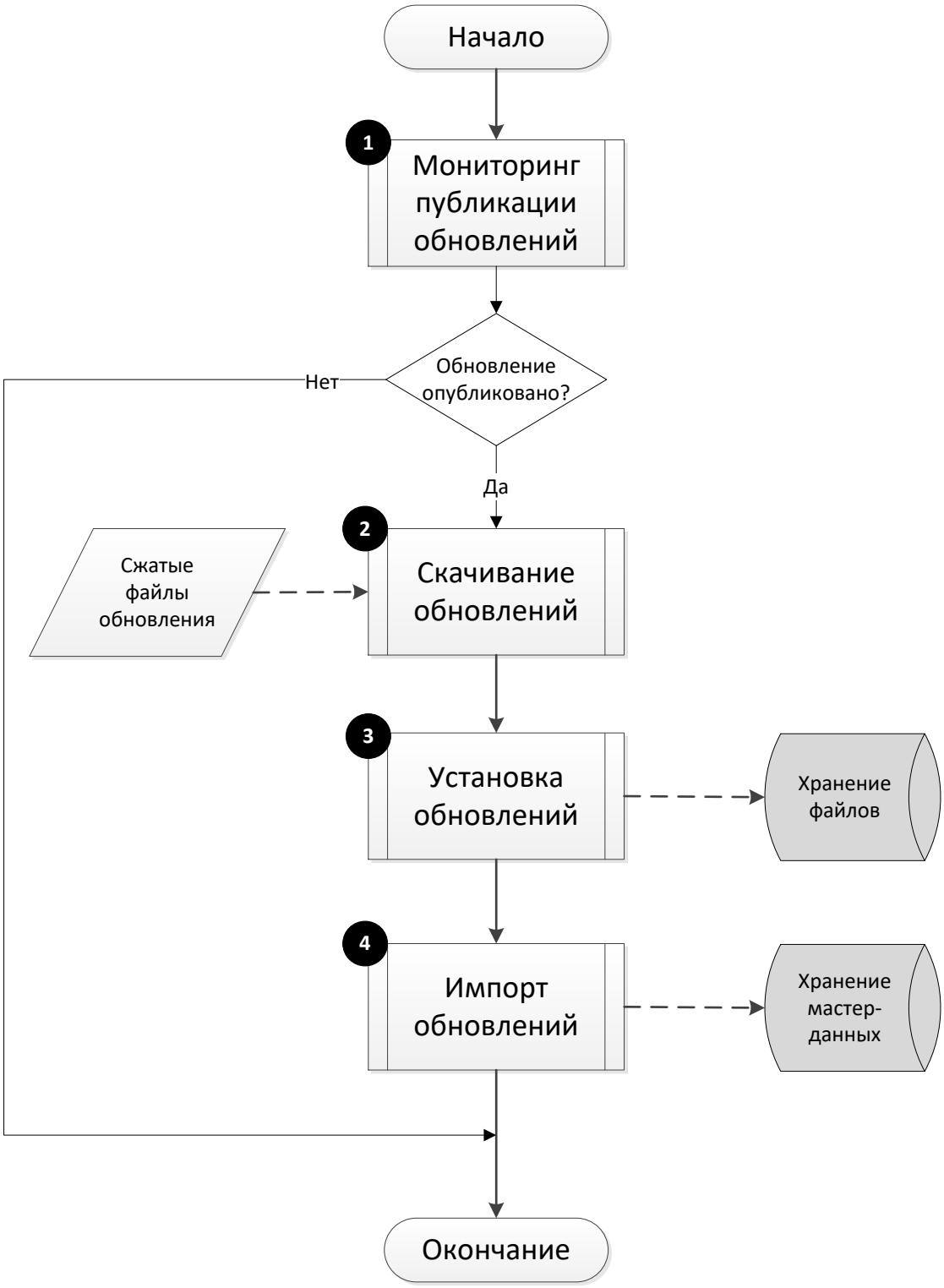

Рисунок 10 – Алгоритм обновления

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.

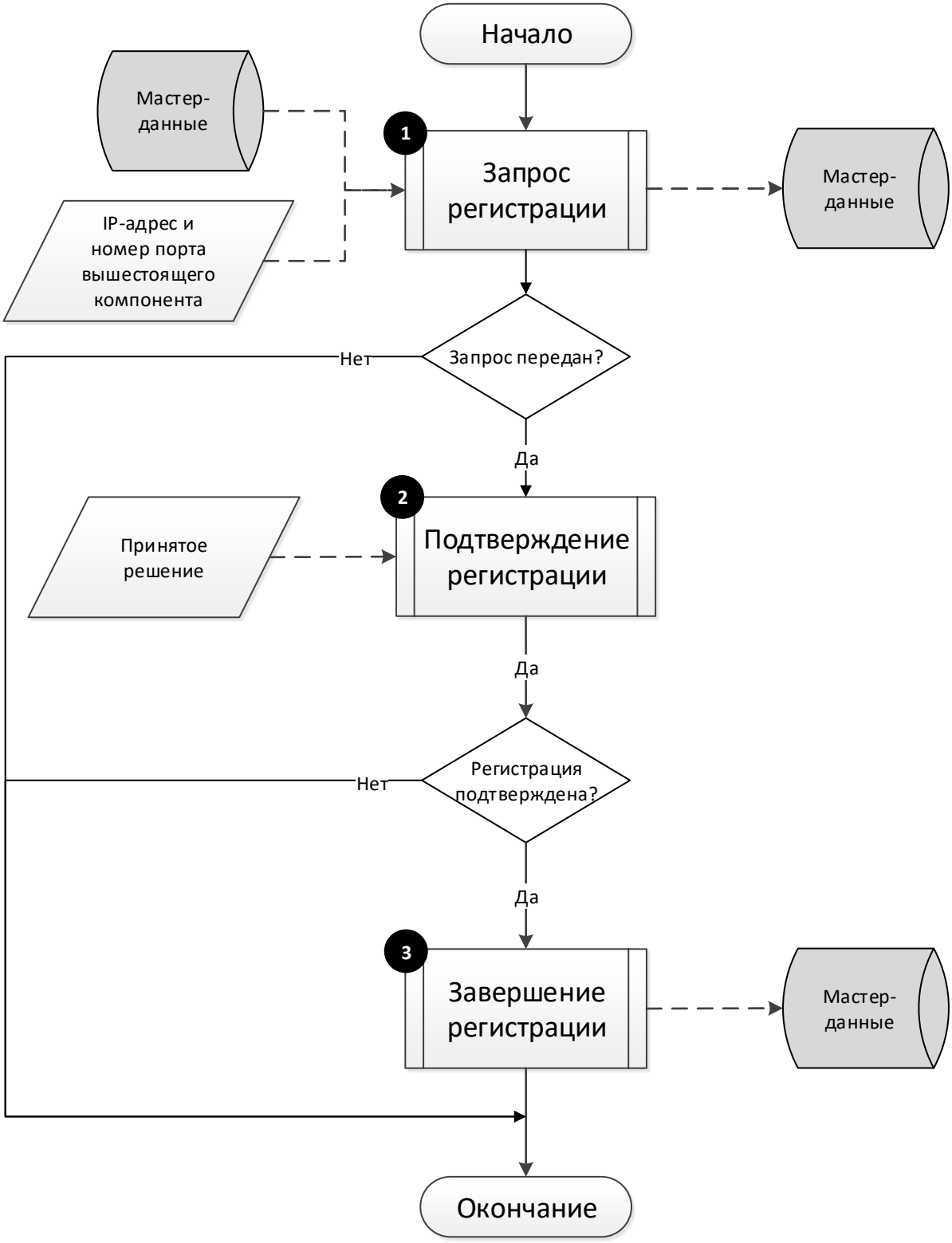

Рисунок 11 – Алгоритм регистрации компонента

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. Подробно алгоритмы и программный интерфейс взаимодействия описаны в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С

3.5.11 Алгоритм регистрации на сервере обновлений

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

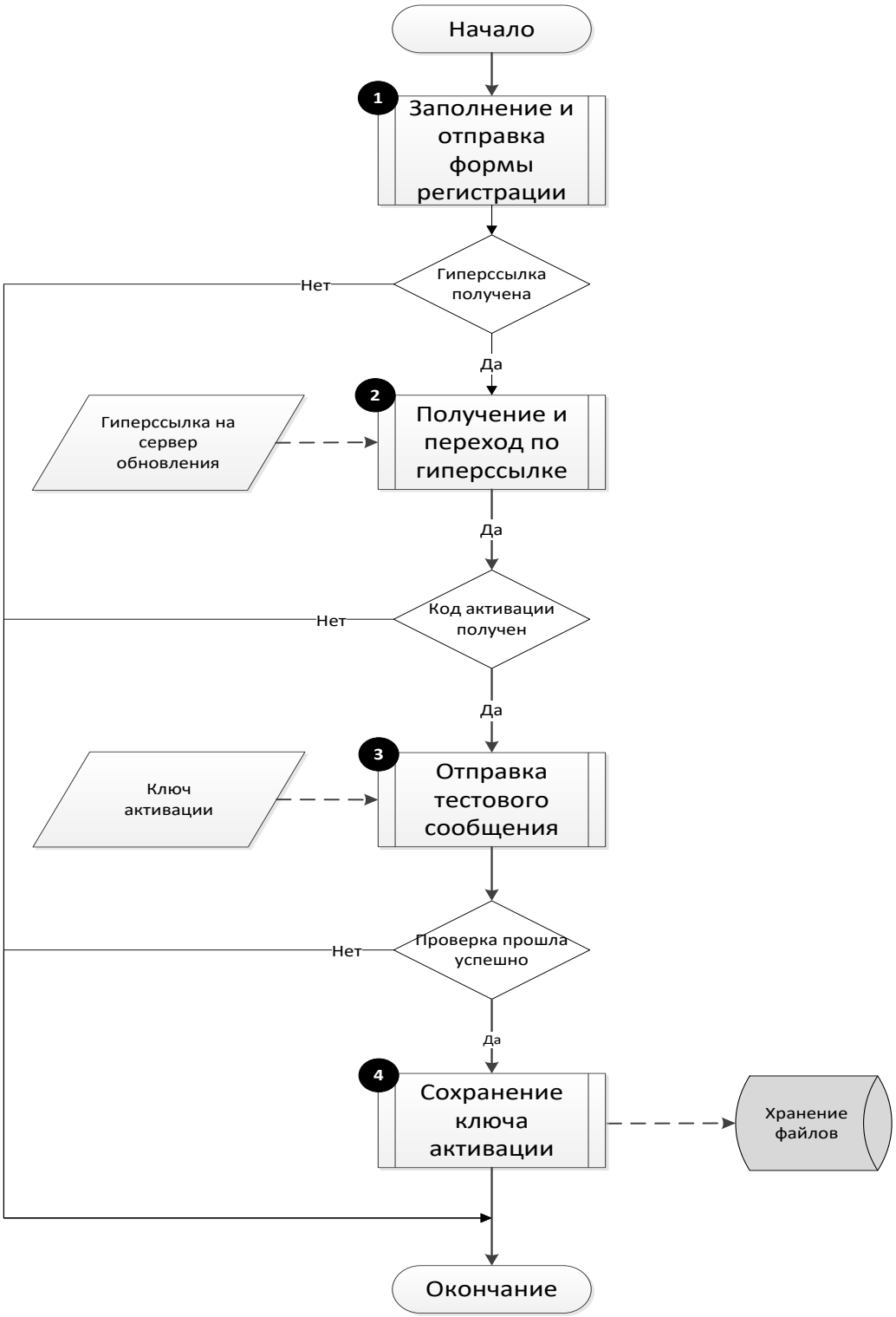

Рисунок 12 – Алгоритм регистрации на сервере обновлений

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 3). Модуль «Эвристический анализ» работает в режиме обнаружения.

– Обучение. В этом состоянии в ПС Сенсор запущены все модули (см. раздел 3.3 Таблица 3). 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 3). 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.

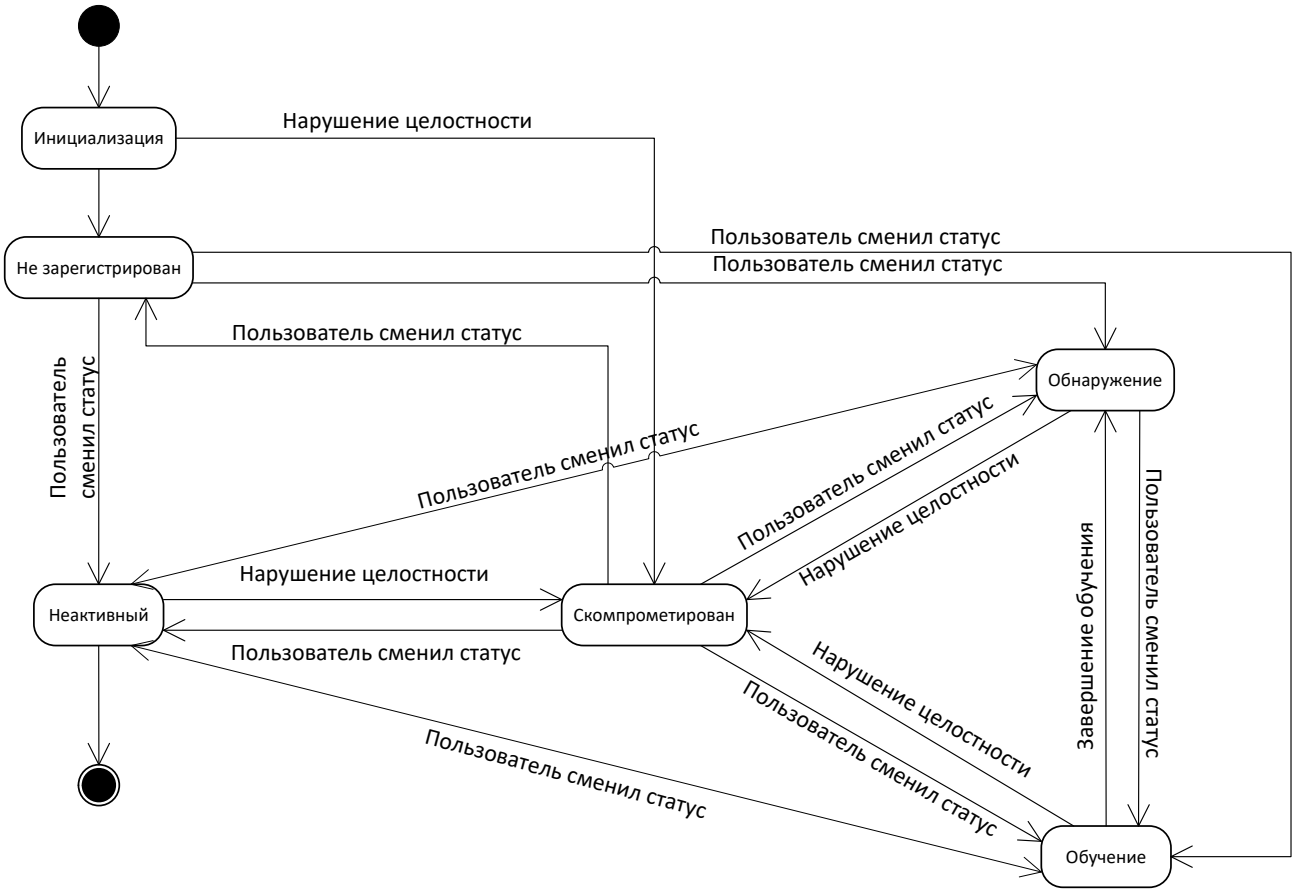

Рисунок 13 – Схема смены статусов ПС Сенсор

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:

г) Выполнение команд,

д) Мониторинг состояний,

е) 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 3).

– 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 3). В этом состоянии Модуль «Обновление» не выполняет обновление справочников «Пользователи» и «Роли пользователей».

На рисунке 14 представлена схема смены статусов ПС СУС.

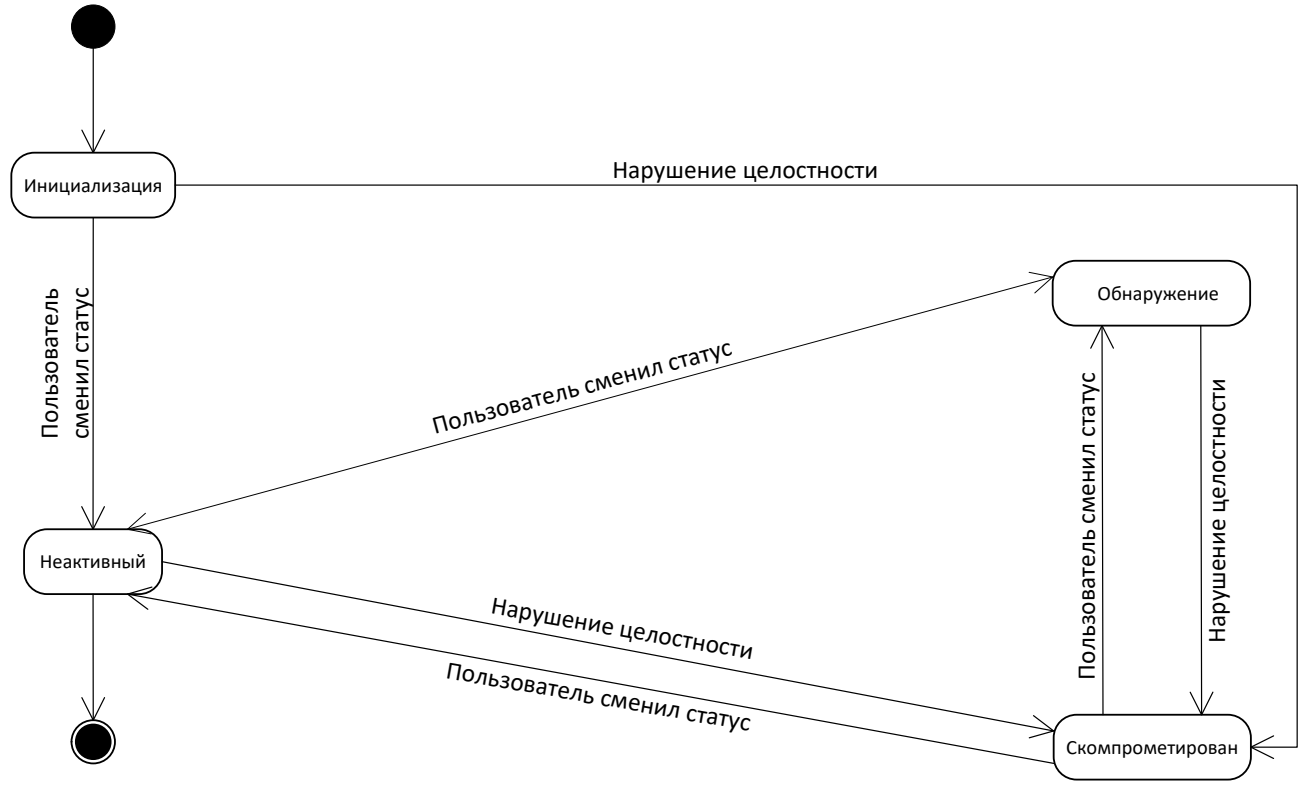

Рисунок 14 – Схема смены статусов ПС СУС

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 4.

Таблица 4 – 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.

6 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

6.1 Виды, формат, описание входных и выходных данных

6.1.1 Сетевые пакеты в контролируемом канале передачи данных. Эти сетевые пакеты поступают на сетевой интерфейс сенсора. Формат и метод кодирования пакетов определены в RFC 791.

6.1.2 События информационной безопасности. СИБ появляются в ПС Сенсор. Хранение СИБ в БД ПС ПК СОВ обеспечивает модуль «Хранение больших данных». Структура и атрибутивный состав данных представлен в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. СИБ передаются вверх по иерархии компонентов (используется модуль «Передача и приём данных и команд»). Передача СИБ выполняется в пакетном режиме с учётом приоритета: СИБ с более высоким уровнем критичности и с большей датой создания отправляются на вышестоящий ПС СУС в первую очередь. Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С. Число СИБ в пакете является настраиваемой величиной.

6.1.3 Копия трафика. Создаётся в ПС Сенсор в виде PCAP-файлов. PCAP-файл содержит информацию: о сетевом пакете, вызвавшем срабатывание решающего правила; десяти предыдущих сетевых пакетах и десяти пакетах после этого пакета – при их наличии в сетевом соединении. Файлы передаются из ПС Сенсор вверх по иерархии компонентов (используется модуль «Передача и приём данных и команд»). Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.4 Обновление. Представляет собой набор файлов обновлений. Каждый вид обновления поступает в своём файле в сжатом виде. Имена файлов имеют структуру: pluton-update-<YYYYMMDD[N]>-<tag>.tar.gz, где:

– YYYYMMDD – дата обновления;

– N – номер обновления в указанной дате;

– tag – тип обновления (SOFTWARE_UPDATE, SURICATA_UPDATE, BRO_UPDATE, BRO_SIG_UPDATE, BL_UPDATE, GEOIP_UPDATE, MAP_UPDATE, VUL_UPDATE).

Обновление поступает из сервера обновлений на корневой ПС СУС и далее распространяется вниз по иерархии компонентов. Для защиты файлов обновлений от искажений используется контроль целостности.

6.1.4.1 Обновление программного обеспечения ПС Сенсор – SOFTWARE_UPDATE. Представляет собой набор сжатых бинарных файлов.

6.1.4.2 База решающих правил сигнатурного анализа – SURICATA_UPDATE, BRO_SIG_UPDATE. Хранение базы решающих правил сигнатурного анализа в БД ПС ПК СОВ обеспечивает модуль «Хранение мастер-данных». Также база решающих правил располагается в виде набора текстовых файлов в модуле «Хранение файлов» ПС Сенсор. Формат представления информации внутри указанных файлов соответствует формату сигнатурных решающих правил СОА Suricata, СОА Bro, утилиты p0f, которые определены официальными документами, размещёнными на интернет-ресурсах https://suricata-ids.org, https://www.bro.org/, lcamtuf.coredump.cx/p0f/.

6.1.4.3 Программные сценарии эвристического анализа – BRO_UPDATE. Хранятся в ПС Сенсор в виде текстовых файлов в модуле «Хранение файлов» и используются СОА Bro.

6.1.4.4 Чёрные списки – BL_UPDATE. Предназначены для обнаружения в сетевом трафике объектов из чёрных списков: IP-адреса, адрес электронной почты, DNS-имя, URL-адрес, MD5-хеш файла. Чёрные списки хранятся в ПС Сенсор в виде текстовых файлов в модуле «Хранение файлов» и используются СОА Bro. Хранение чёрных списков в БД ПС ПК СОВ обеспечивает модуль «Хранение мастер-данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

6.1.4.5 База GeoIP – GEOIP_UPDATE. База GeoIP предназначена для связывания IP-адресов выявленных объектов КА, хостов источников угроз, хостов контролируемой системы, компонентов ПК СОВ с их географическим местоположением. Хранение данных в виде бинарных файлов в ПС ПК СОВ обеспечивает модуль «Хранение файлов».

6.1.4.6 Данные картографии – MAP_UPDATE. Предназначены для представления местоположения выявленных объектов КА, хостов источников угроз, хостов контролируемой

системы, компонент ПК СОВ на географической карте в модуле «Графический пользовательский интерфейс». Данные картографии хранятся в виде файлов формате SpatialDB и файлов в формате MapServer. Хранение данных обеспечивает модуль «Хранение файлов».

6.1.4.7 База уязвимостей – VUL_UPDATE. В ПС ПК СОВ программное обеспечение хостов контролируемых систем соотносится с базой уязвимостей. Данные базы уязвимостей используются для оценки уязвимости хостов и расчёта индикатора достоверности угрозы. База уязвимости хранится в БД ПС ПК СОВ посредством модуля «Хранение мастер-данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В.

6.1.5 Конфигурационные параметры работы ПС ПК СОВ. Хранятся в текстовых конфигурационных файлах в локальной файловой системе среды функционирования ПС ПК СОВ. Хранение обеспечивает модуль «Хранение файлов». Местоположение конфигурационных файлов представлено в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81, Приложение А.

К конфигурационным параметрам относятся:

- 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.

Для установки значений конфигурационных параметров в конфигурационных файлах, а также установки необходимых настроек среды функционирования в ПС ПК СОВ применяется командная среда ОС. Командная среда предоставляет доступ к возможностям диагностики и настройки ПС ПК СОВ. Команды, доступные в командной среде ОС, их формат и примеры использования приведены в документах "ПС «Сенсор-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.183-01 32 и "ПС «СУС-Плутон-М1.0». Руководство системного программиста", ДБАР.62.01.12.000.182-01 32. Не предусматривается изменение содержимого файлов конфигурации пользователем или иными программными средствами,

кроме как посредством командной среды ОС или восстановлением из резервной копии с внешнего носителя.

6.1.6 Управляющие команды со стороны ПС СУС. К таким командам относятся:

– зарегистрировать компонент;

– запустить обучение;

– завершить обучение;

– активировать сенсор;

– деактивировать сенсор;

– активировать/деактивировать решающие правила;

– подтвердить профиль хоста и ПО профиля хоста;

– установить параметры контролируемой системы, в том числе переменные, которые используются в правилах сигнатурного анализа;

– запустить обновления базы контроля целостности;

– запустить контроль целостности;

– зарегистрировать сервер обновлений.

Передачу команд обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.7 Справочные данные. К ним относятся:

– уровни критичности;

– протоколы;

– типы событий информационной безопасности;

– категории событий информационной безопасности;

– типы событий аудита безопасности;

– подразделения;

– страны мира;

– пользователи ПК СОВ;

– роли пользователей ПК СОВ

– типы обновлений;

– типы чёрных списков.

Хранение справочных данных в БД ПС ПК СОВ обеспечивает модуль «Хранение мастер-данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. Справочные данные ведутся в корневом ПС СУС. и передаются вниз по иерархии компонентов. Передачу обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.8 Уведомления. Содержат информацию:

– о зарегистрированных сетевых вторжениях;

– о событиях аудита безопасности, включая: выполнение управляющих команд, выполнение обновлений базы решающих правил сигнатурного анализа, выполнение обновлений чёрных списков, изменение параметров функционирования сенсора, а также параметров функционирования технических средств и ОС.

Уведомления передаются пользователям ПК СОВ электронной почтой.

6.1.9 Статистические данные трафика. Представляют собой статистические характеристики потоков трафика в контролируемом канале передачи данных. Данные появляются в ПС Сенсор и сохраняются в БД. Хранение обеспечивает модуль «Хранение больших данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. Данные передаются из ПС Сенсор вверх по иерархии компонентов. Передачу обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.10 Данные аудита безопасности. К ним относятся события аудита безопасности следующих видов:

– аудит целостности;

– аудит действий пользователей ПК СОВ;

– аудит изменений режимов работы ПС ПК СОВ;

– аудит выполнение программ и процессов ПС ПК СОВ.

Данные аудита безопасности хранятся в БД ПС ПК СОВ. Хранение обеспечивает модуль «Хранение больших данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. События аудита безопасности передаются вверх по иерархии компонентов по запросу ПС СУС. Передачу обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.11 Данные о состоянии и работоспособности. Содержат информацию о параметрах функционирования ПС ПК СОВ:

– процент использования ОЗУ;

– процент использования ЦПУ;

– процент использования файла подкачки;

– процент использования НЖМД;

– признак компрометации ПС ПК СОВ.

ПС ПК СОВ собирает данные с помощью программы-агента Net-SNMP. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix, входящее в состав поставки ПК СОВ. Хранение данных в БД ПС ПК СОВ обеспечивает модуль «Хранение мастер-данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. Данные передаются вверх по иерархии компонентов. Передачу обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.12 Профили хостов. Данные хостов представляют собой информацию о найденных ПС Сенсор хостах в процессе обучения и обнаружения:

- тип, имя, адрес, статус, важность, контролируемую систему;
- показатели сетевой активности и статистику сетевого трафика;
- установленные программные продукты и связанные с ними уязвимостями;
- перечень пользователей;
- историю изменений.

Данные появляются в ПС Сенсор и сохраняются БД ПС Сенсор. Хранение обеспечивает модуль «Хранение мастер-данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. Данные передаются вверх по иерархии компонентов. Передачу обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.13 Журналы событий СОА. Дополнительные данные, которые создают СОА Bro в результате обработки сетевого трафика, позволяющие предоставить расширенную информацию для анализа СИБ. Записи журналов событий СОА появляются в ПС Сенсор и сохраняются в БД. Сохранение данных обеспечивает модуль «Хранение больших данных». Структура и атрибутивный состав данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение В Описание структуры базы данных", ДБАР.62.01.12.000.181-01 81-В. Данные передаются по запросу в ПС СУС. Передачу обеспечивает модуль «Передача и приём данных и команд». Формат и метод кодирования передаваемых данных определены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка. Приложение С Описание программного интерфейса взаимодействия компонентов", ДБАР.62.01.12.000.181-01 81-С.

6.1.14 Данные для SIEM-систем. Данные о СИБ в формате CEF, которые создёт ПС Сенсор с помощью сервиса rsyslog. Данные предназначены для внешних SIEM-систем

6.2 Характер, организация и предварительная подготовка входных и выходных данных

Характер, организация и предварительная подготовка данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81.

6.3 Формат, описание и способ кодирования входных и выходных данных

Формат, описание и способ кодирования входных и выходных данных представлены в документе "ПК «СОВ «Плутон-М1.0». Пояснительная записка", ДБАР.62.01.12.000.181-01 81.

6.4 Входные данные ПС Сенсор

6.4.1 Сетевые пакеты в контролируемом канале передачи данных.

6.4.2 Обновления:

- база решающих правил сигнатурного анализа;
- чёрные списки;
- программные сценарии эвристического анализа;
- программное обеспечение сенсора;
- база GeoIP;
- база уязвимостей;
- справочные данные.

6.4.3 Управляющие команды со стороны СУС

6.4.4 Конфигурационные параметры.

6.4.5 Профили хостов.

6.5 Выходные данные ПС Сенсор

6.5.1 СИБ.

6.5.2 Копия трафика.

6.5.3 Журналы событий СОА.

6.5.4 Статистические данные трафика.

6.5.5 Профили хостов.

6.5.6 Данные аудита безопасности.

6.5.7 Данные о состоянии и работоспособности.

6.5.8 Уведомления.

6.5.9 Данные для SIEM-систем.

6.6 Входные данные ПС СУС

6.6.1 СИБ.

6.6.2 Копия трафика.

6.6.3 Журналы событий СОА.

6.6.4 Статистические данные трафика.

6.6.5 Профили хостов.

6.6.6 Данные аудита безопасности.

6.6.7 Данные о состоянии и работоспособности.

6.6.8 Обновления:

- база решающих правил сигнатурного анализа;
- чёрные списки;
- программное обеспечение;
- база GeoIP;
- данные картографии;
- база уязвимостей;
- справочные данные.

6.6.9 Управляющие команды со стороны вышестоящего ПС СУС.

6.6.10 Конфигурационные параметры.

6.7 Выходные данные ПС СУС

6.7.1 СИБ.

6.7.2 Копия трафика.

6.7.3 Журналы событий СОА.

6.7.4 Статистические данные трафика.

6.7.5 Профили хостов.

6.7.6 Данные аудита безопасности.

6.7.7 Данные о состоянии и работоспособности.

6.7.8 Обновления:

– база решающих правил сигнатурного анализа;

– чёрные списки;

– программное обеспечение;

– база GeoIP;

– данные картографии;

– база уязвимостей;

– справочные данные.

6.7.9 Управляющие команды в сторону подчинённых компонентов.

6.7.10 Уведомления.

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					