

УТВЕРЖДЕНО

18678659.00001-03 31 02-ЛУ

**ПРОГРАММНЫЙ КОМПЛЕКС
РЕТРОСПЕКТИВНОГО АНАЛИЗА СЕТЕВОГО ТРАФИКА
«СТЕТОСКОП» ВЕРСИИ 3.0**

Описание применения

18678659.00001-03 31 02

Инд. № подл.	Подп. и дата	Взам. инв. N	Инд. N дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ 18678659.00001-03 31 02 является описанием применения Программного комплекса ретроспективного анализа сетевого трафика «Стетоскоп» версии 3.0 (далее - ПК Стетоскоп).

В документе приводится общее описание ПК Стетоскоп, варианты исполнения и поставок, области применения, типовая схема подключения, способы коммуникации с ПК Стетоскоп, описаны основные возможности сценариев задания политик безопасности, перечислены возможности по анализу сетевого трафика, возможности анализа накопленной статистики с целью выявления атак и аномалий сетевого трафика, возможности управления ПК Стетоскоп с использованием встроенного WEB-приложения, а также функциональные возможности по администрированию ПК Стетоскоп.

СОДЕРЖАНИЕ

1. Общие сведения.....	4
1.1. Назначение ПК Стетоскоп	4
1.2. Варианты исполнения и поставок ПК Стетоскоп.....	4
1.3. Схема подключения ПК Стетоскоп.....	6
1.4. Архитектура ПК Стетоскоп	9
1.4.1 Общее описание ПК Стетоскоп	9
1.4.2 Способы коммуникации с ПК Стетоскоп	11
1.4.3 Экспорт сообщений	12
2. Описание функциональных возможностей ПК Стетоскоп.....	14
2.1. Системные возможности.....	14
2.2. Возможности встроенных анализаторов.....	14
Перечень принятых сокращений.....	16
Лист регистрации изменений	17

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение ПК Стетоскоп

ПК Стетоскоп, предустановленный на аппаратную платформу или гостевую виртуальную машину (далее – АПК Стетоскоп или изделие), предназначен для захвата, записи и индексации сетевого трафика, анализа передаваемых по сети данных с целью выявления атак и аномалий, сбора и визуализации статистики сетевых сессий и передаваемых данных, выявление используемых сетевых протоколов, форматов и служб, определение географической принадлежности и DNS-имен IP-адресов взаимодействующих сетевых субъектов, экспорта по требованию оператора образцов сетевого трафика и перенаправления сетевого трафика на внешние анализаторы, перенаправление системных событий и событий информационной безопасности (далее – ИБ) на внешние системы обработки событий (к примеру, системы мониторинга и управления ИБ, SIEM-системы).

1.2. Варианты исполнения и поставок ПК Стетоскоп

ПК Стетоскоп предназначен для исполнения на серверах архитектуры Intel x86-64 или на гостевых виртуальных машинах эмулирующих архитектуру Intel x86-64 под управлением операционной системы семейства Linux.

В зависимости от характеристик аппаратной платформы ПК Стетоскоп позволяет обрабатывать сетевой поток на скорости до 10 Гбит/с в каждом направлении сетевого трафика (т.е. суммарно до 20 Гбит/с)

Для обработки сетевых потоков на скорости до 10 Гбит/с в каждом направлении (суммарно 20 Гбит/с) рекомендуются следующие параметры аппаратной платформы:

18678659.00001-03 31 02

- сервер в корпусе 19”, монтируемом в стандартную коммуникационную стойку;
- оперативная память не менее 256 ГБ;
- постоянно запоминающее устройство (далее - ПЗУ) №1 для операционной системы не менее 64 ГБ;
- ПЗУ №2 для хранения индекса и событий журналов аудита не менее 4 ТБ;
- ПЗУ №3 для хранения образцов записанного трафика суммарно не менее 120 ТБ (Расширение объема ПЗУ №3 позволит увеличить срок хранения образцов записанного трафика);
- поддержка ядра Linux версии 4 и выше;
- один сетевой интерфейс, работающий на скорости не менее 1 Гб/с, для реализации канала управления. Для реализации отказоустойчивого канала управления рекомендуется выделять два сетевых интерфейса для реализации канала управления;
- один и более сетевых интерфейсов с чипсетами Intel, работающих на скорости 10 Гбит/с для захвата трафика.

Для обработки сетевых потоков на скорости до 1 Гбит/с в каждом направлении (суммарно 2 Гбит/с) рекомендуются следующие параметры аппаратной платформы:

- сервер в корпусе 19”, монтируемом в стандартную коммуникационную стойку;
- оперативная память не менее 64 ГБ;
- постоянно запоминающее устройство (далее - ПЗУ) №1 для операционной системы не менее 64 ГБ;
- ПЗУ №2 для хранения индекса и событий журналов аудита не менее 256 ГБ;

- ПЗУ №3 для хранения образцов записанного трафика суммарно не менее 12 ТБ (Расширение объема ПЗУ №3 позволит увеличить срок хранения образцов записанного трафика);
- поддержка ядра Linux версии 4 и выше;
- один сетевой интерфейс, работающий на скорости не менее 1 Гб/с, для реализации канала управления. Для реализации отказоустойчивого канала управления рекомендуется выделять два сетевых интерфейса для реализации канала управления;
- один и более сетевых интерфейсов с чипсетами Intel, работающих на скорости 1 Гбит/с для захвата трафика.

1.3. Схема подключения ПК Стетоскоп

Исходными данными для ПК Стетоскоп являются потоки сетевого трафика. ПК Стетоскоп выполняет обработку потоков сетевого трафика путем индексации и анализа. Для решения задач индексации и анализа потоки сетевого трафика должны быть записаны в формате PCAP.

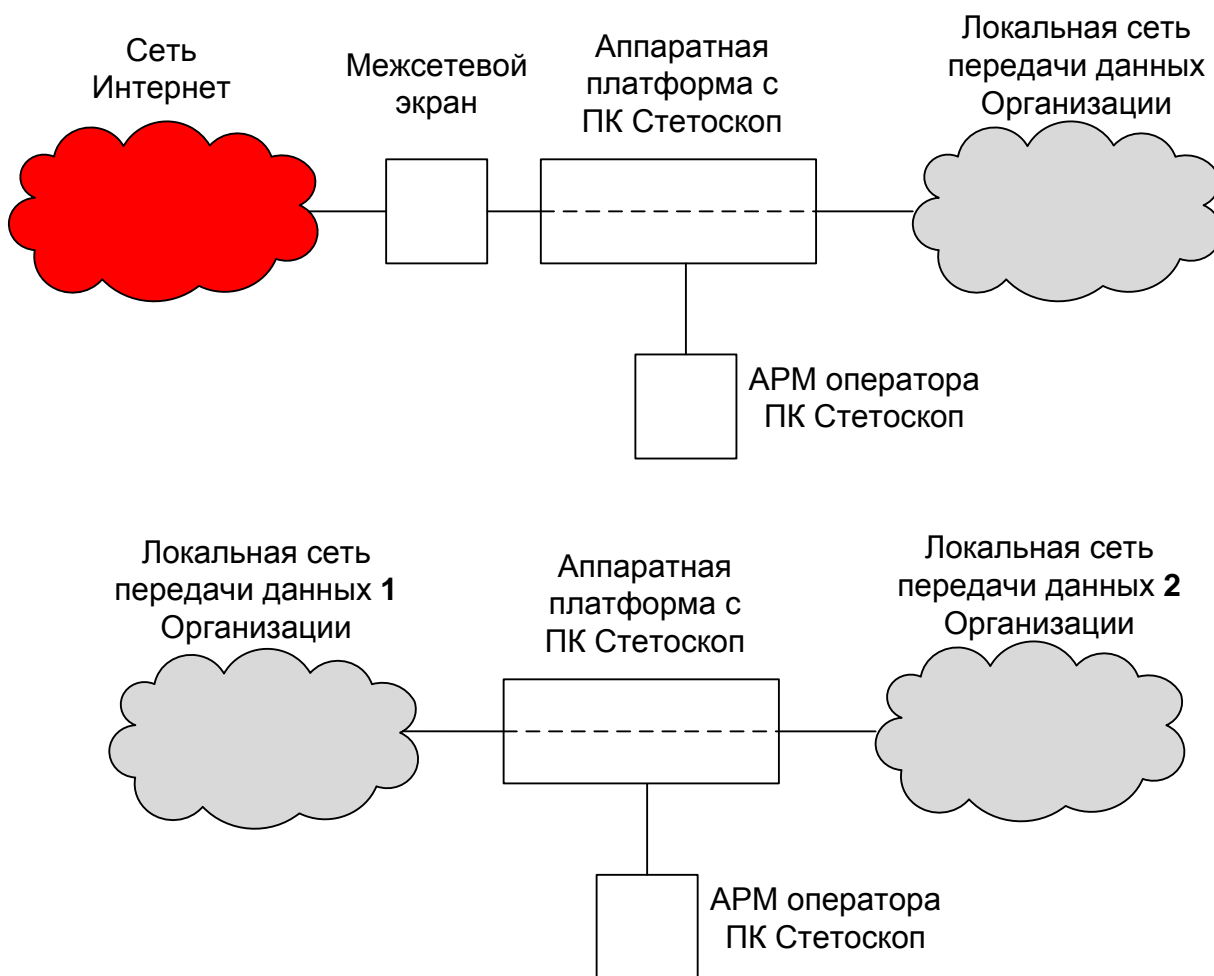
ПК Стетоскоп обладает собственным функционалом захвата и записи потоков сетевого трафика в формате PCAP. Для захвата потоков сетевого трафика необходимо интегрировать АПК в действующую сеть передачи данных контролируемой информационной системы (далее – ИС) Организации. Для этого предусмотрены два режима встраивания: режим «мост» и режим «ответвитель».

Режим «мост» подразумевает встраивание АПК в разрыв действующей линии передачи данных контролируемой ИС Организации. В этом режиме используется два сетевых интерфейса АПК, которые разрывают действующую линию связи, и выполняется настройка АПК по пробросу (перекладыванию) входящих пакетов из одного интерфейса в другой. Типовая схема включения в режиме «мост» подразумевает установку АПК

либо между двумя локальными сегментами сети передачи данных Организации, либо между локальным сегментом и сетью Интернет.

В процессе проброса сетевых пакетов между двумя сетевыми интерфейсами АПК, их копии захватываются ПК Стетоскоп и записываются на локальный диск АПК с последующим анализом. Данный режим при штатной работе АПК не оказывает влияние на линию связи, в которую он встроен. Для обеспечения отказоустойчивости линии связи к возможным аппаратным и/или программным сбоям АПК рекомендуется применять сетевые платы с функцией bypass. Пример встраивания АПК в действующую линию связи в режиме «мост» представлен на рисунке 1.

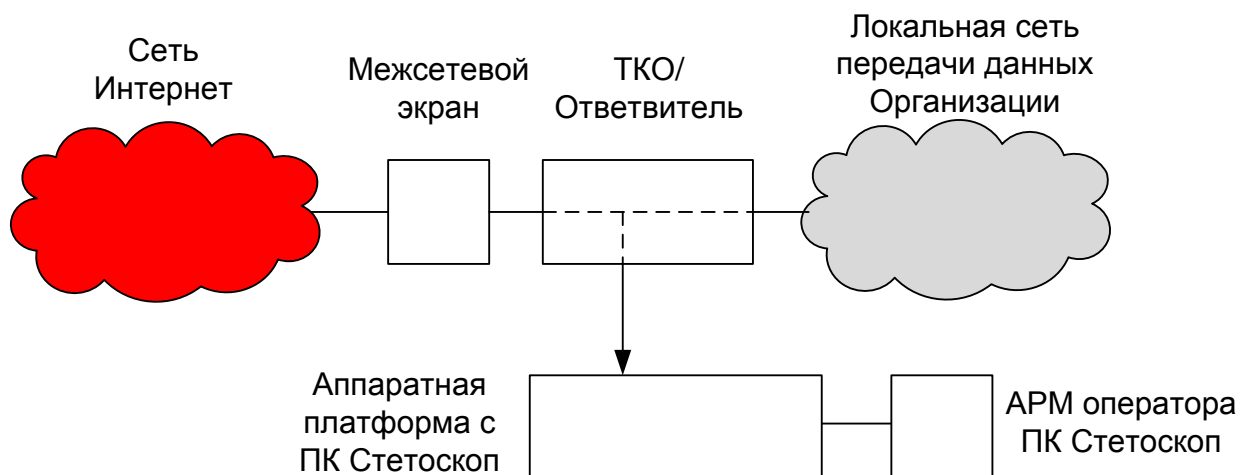
Рисунок 1. Схема применения режима встраивания «мост».



Режим «ответвитель» подразумевает встраивание АПК либо через устройство ответвления трафика (TAP), либо через подключение к порту

зеркалирования (port mirroring или span-порт) сетевого трафика используемого телекоммуникационного оборудования (далее – ТКО). В этом режиме ПК Стетоскоп захватывает копии сетевых пакетов, записывает их на локальный диск АПК с последующим анализом, не разрывая линию связи, а получая их с ТАР-устройства или с порта зеркалирования ТКО. В режиме «ответвитель» АПК Стетоскоп может захватывать сетевые потоки циркулирующие между двумя локальными сегментами сети передачи данных Организации, между локальным сегментом и сетью Интернет или между локальными узлами ИС Организации.

Рисунок 2. Схема применения режима встраивания «ответвитель».



В случае применения режима «ответвитель» путем настройки порта зеркалирования копирования входящих и исходящих сетевых пакетов с нескольких портов ТКО в один порт анализа необходимо учитывать емкость выбранного порта ТКО для подключения АПК, чтобы не превысить пропускную способность исходящих сетевых потоков, иначе могут быть потери сетевых пакетов на ТКО.

ПК Стетоскоп может выполнять анализ ранее записанных сетевых потоков в формате PCAP. Для этого необходимо выполнить копирование на АПК файлов в формате PCAP, ранее записанных сетевых потоков, и провести процедуру регистрации этих файлов в ПК Стетоскоп.

Независимо от способа получения PCAP-файлов (собственным механизмом захвата или копированием ранее записанного трафика) ПК Стетоскоп выполняет индексацию и анализ сетевых потоков, записанных в PCAP-файлах. Скорость индексации и анализа зависит от конфигурации АПК и сложности применяемых алгоритмов анализа. Используя рекомендованные параметры аппаратной платформы или гостевой виртуальной машины для исполнения ПК Стетоскоп скорость индексации и анализа должна быть не менее скорости записи потоков сетевого трафика.

Результатом анализа потоков сетевого трафика являются сообщения о событиях ИБ, которые записываются во встроенную базу данных (БД) и при необходимости могут быть перенаправлены на внешних получателей событий ИБ по протоколу SYSLOG.

1.4. Архитектура ПК Стетоскоп

1.4.1 Общее описание ПК Стетоскоп

В состав ПК Стетоскоп входят следующие программные средства (далее по тексту – ПС):

- ПС «Дампер»;
- ПС «Индексатор»;
- ПС «Анализатор»;
- ПС «Клиент»;
- ПС «Ротатор»;
- ПС «База данных» (далее по тексту – ПС «БД»).

ПС «Дампер» предназначено для гарантированного захвата сетевых пакетов на скорости до 20 Гбит/с, записи их на диск и передачи для дальнейшей обработки ПС «Индексатор».

ПС «Индексатор» предназначено для обработки сетевых пакетов на скорости до 20 Гбит/с в режиме близком к реальному времени, записи

информации о них в ПС «БД» и передачи информации о потоках сетевого трафика на дальнейшую обработку в ПС «Анализатор».

Обработка сетевых пакетов включает в себя следующие операции:

- объединение (склейка) сетевых пакетов в сетевые сессии;
- индексация сетевых пакетов и сетевых сессий по множественным атрибутам;
- расчет сетевой статистики по пакетам и сессиям;
- выявление протоколов, форматов и служб;
- определение географической принадлежности и DNS-имен по IP-адресам взаимодействующих сетевых субъектов;
- выявление отклонений от стандартов обмена (RFC) в обнаруженных сетевых протоколах.

ПС «Анализатор» предназначено для выполнения поиска по заданным правилам атак и аномалий в сетевом трафике различными методами, в том числе методами с применением машинного обучения. ПС «Анализатор», получая данные от ПС «Индексатор» и от ПС «БД» выполняет следующие виды анализа:

- анализ статистики трафика на предмет превышения порогов по различным метрикам и группировкам;
- анализ сетевых субъектов по IP-адресам или DNS-именам на предмет их вхождения в особые («плохие») списки;
- Выявление запрещенных протоколов или выявление новых протоколов для контролируемой ИС;
- Выявление запрещенных или новых для контролируемой ИС серверных сетевых портов;
- Выявление новых IP-адресов для контролируемой ИС;

ПС «Клиент» предназначено для предоставления оператору средств управления и мониторинга работой ПК Стетоскоп и решения операторских задач по мониторингу трафика и событий ИБ.

ПС «БД» предназначена для хранения и выдачи по запросу образцов трафика, статистики трафика, посчитанной по записанным образцам трафика, системных событий, генерируемых ПС в процессе работы, и событий ИБ, генерируемых ПС «Анализатор» на основании заданных правил анализа.

ПС «Ротатор» предназначено для выполнения в автоматическом режиме задач управления свободным местом дискового пространства АПК. По заранее заданным конфигурационным параметрам ПС «Ротатор» на регулярной основе следит за оставшимся свободным местом и обеспечивает бесперебойную работу ПК Стетоскоп в режиме 24/7 без необходимости обслуживания АПК персоналом путем ротации и архивации накопленных данных.

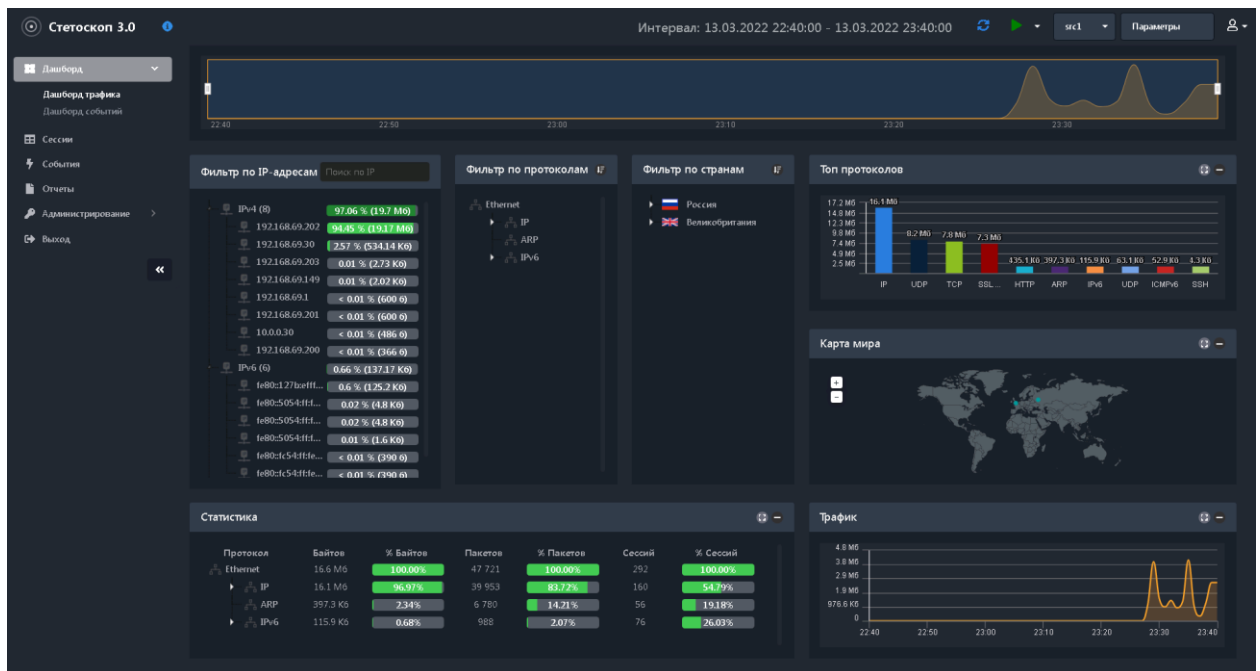
1.4.2 Способы коммуникации с ПК Стетоскоп

Для управления и администрирования ПК Стетоскоп доступны два канала управления: локальный терминал сервера и сетевой интерфейс (Ethernet). По каналу Ethernet возможен доступ по протоколам SSH, HTTP(s) (WEB-интерфейс). Для администрирования

WEB-интерфейс предназначен для эффективной удалённой операторской деятельности с ПК Стетоскоп через WEB-браузер. WEB-интерфейс упрощает работу оператора. Один из образов консоли управления в рассматриваемом режиме приведён на рисунке 1. Кроме операторской деятельности WEB-интерфейс позволяет решать некоторые задачи администрирования:

- управление пользователями, которым предоставлен доступ к WEB-интерфейсу,
- мониторинг состояния системных и прикладных служб изделия.

Рисунок 3. Образец интерфейса WEB-приложения управления.



Локальный терминал или сетевой интерфейс по протоколу SSH предназначен в изделии для решения функций администрирования:

- задание правил для анализаторов,
- управление службой захвата трафика и сетевыми интерфейсами захвата,
- управления службой журнала аудита по сохранению системных сообщений и сообщений аудита сетевого трафика в локальных журналах изделия и пересылки событий на внешние анализаторы,
- управление службами индексации и анализа трафика,
- управление вспомогательными службами по обслуживанию непрерывной работы изделия (24/7).

1.4.3 Экспорт сообщений

ПК Стетоскоп поддерживает экспорт системных сообщений и сообщений от анализаторов во внешние системы обработки событий (SIEM,

комплекс программных средств системы регистрации, анализа и мониторинга событий информационной безопасности производства ООО «ЦСС»).

Данный функционал реализуется по средствам протокола SYSLOG и позволяет гибко настраивать параметры экспорта.

Изделие поддерживает экспорт накопленных данных во внешние системы с применением общедоступных протоколов: HTTP(s), SAMBA. Накопленными данными являются:

- файлы записанного трафика,
- статистика трафика,
- события анализаторов трафика и статистики трафика.

2. ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ПК СТЕТОСКОП

2.1. Системные возможности

ПК Стетоскоп предоставляет пользователю интерфейс изучения захваченного и проиндексированного трафика на предмет аномалий и атак. Для решения этих задач предусмотрены агрегационные отчеты и табличные представления статистики сетевого трафика с возможностью поиска и фильтрации. Агрегационные отчеты включают представление сетевого трафика на временной шкале с указанием количественных характеристик – интенсивность трафика, на круговых и столбчатых диаграммах – распределение трафика по заданным параметрам. Захваченный сетевой трафик агрегируется по сетевым протоколам, сетевым адресам, географической принадлежности, а также ведется расчет количественных показателей по объему, количеству пакетов и сетевых сессий. На основании этих данных оператор ПК Стетоскоп может исследовать в автоматизированном режиме сетевой трафик на предмет аномалий, связанных с количественными показателями подсетей и индивидуальных хостов локальных и внешних хостов.

Для автоматического анализа трафика предусмотрен набор анализаторов, которые выполняют обработку статистики сетевого трафика на предмет наличия в нем аномалий по заранее заданным алгоритмам, которые настраиваются пользователем с учетом потоков данных информационной системы.

2.2. Возможности встроенных анализаторов

ПС «Анализатор» отвечает за анализ статистики сетевых потоков, поступающих от ПС «Индексатор», на предмет выявления аномалий и нарушений, заданных специальными фильтрами.

ПС «Анализатор» выполняет анализ статистики сетевых потоков на основе фильтров, заданных в файлах конфигурации в формате JSON.

Конфигурация включает в себя возможность задания расписания работы фильтров анализатора, количественные показатели и параметры агрегации.

В случае обнаружения ПС «Анализатор» условий, заданных в фильтрах, генерируется и отправляется в БД и системный журнал аудита событий соответствующее сообщение.

ПС «Анализатор» поддерживает два режима работы:

- режим анализа новых данных,
- режим ретроспективного анализа.

Режим анализа новых данных является основным режимом работы анализатора. Он подразумевает анализ данных, поступающих от ПС «Индексатор» в режиме близком к реальному времени. Эти данные накапливаются в течение всего объявленного в фильтре агрегационного периода; по достижению конца агрегационного периода происходит вывод статистики, а данные сбрасываются.

Ретроспективный режим подразумевает анализ уже имеющихся в БД данных на предмет случившихся в прошлом времени нарушений безопасности. В этом режиме анализатор использует временные метки, полученные в процессе записи файлов трафика.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АИС	–	Автоматизированная информационная система
АРМ	–	Автоматизированное рабочее место
БД	–	База данных

[illegible]