РАЗРАБОТКА ПРЕПРОЦЕССОРА ЛОГ ФАЙЛОВ АППАРАТНЫХ КЛЮЧЕЙ ЛИЦЕНЗИОННОЙ ЗАЩИТЫ SENTINEL

А. А. Морунов, Б. В. Цыганков, Э. Н. Васильев

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

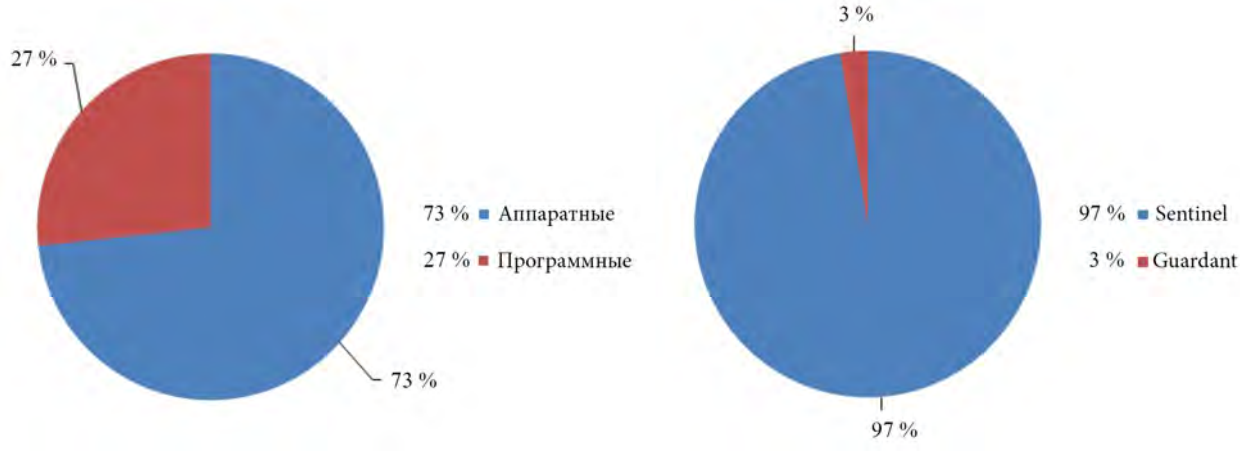
Аппаратные ключи лицензионной защиты Sentinel (АКЛЗ) используются повсеместно производителями программного обеспечения по всему миру, в России один из самых известных производитель ПО, использующий данный вид лицензионной защиты – ЗАО «АСКОН». АКЛЗ – надежные устройства, защищающие от несанкционированного тиражирования ПО. В декабре 2013 года в служебной вычислительной сети (СВС) ВНИИЭФ была введена в эксплуатацию информационная система (ИС) конструкторского проектирования и технической поддержки производства (КП и ТПП), содержащая достаточно большую номенклатуру программных продуктов компании «АСКОН». Компания «АСКОН», начиная с 2010 года, использует систему лицензирования Sentinel HASP от компании SafeNet Inc. Таким образом, анализ информации, полученной после обработки лог файлов АКЛЗ, открывает большие возможности на этапах внедрения и эксплуатации ИС, в качестве средств мониторинга охвата лицензионным ПО рабочих мест пользователей, анализа активности пользователей при проектировании и т. д.

Был проведен анализ существующих средств обработки лог файлов АКЛЗ, в ходе которого выяснилось отсутствие требуемого по функционалу программного обеспечения. Анализ необработанных лог файлов выявил излишнюю перенасыщенность информацией для предполагаемых целей использования. Поиск специализированного ПО для обработки лог файлов АКЛЗ показал, что у компании разработчика – SafeNet Inc. нет открытого (доступного даже на коммерческой основе) инструмента для анализа, поэтому принято решение создать собственный инструмент анализа лог файлов АКЛЗ для подготовки файлов статистических данных.

Актуальность, цели, задачи

В подразделениях ВНИИЭФ используется ПО направления 3D конструкторского проектирования и технологической подготовки производства (направление 3D), защищаемое как программными, так и аппаратными ключами лицензионной защиты, причем зачастую АКЛЗ представлены различными производителями. Результаты анализа средств лицензионной защиты для ПО используемым направлением 3D представлены на рис. 1.

Как видно из рис. 1а в качестве средств лицензионной защиты преимущественно используются АКЛЗ, в свою очередь рисунок 1б демонстрирует,



а б

Рис. 1. Результаты анализа средств лицензионной защиты: а – диаграмма распределения долей аппаратных и программных ключей лицензионной защиты; б – диаграмма распределения долей аппаратных ключей лицензионной защиты производителей Sentinel и Guardant

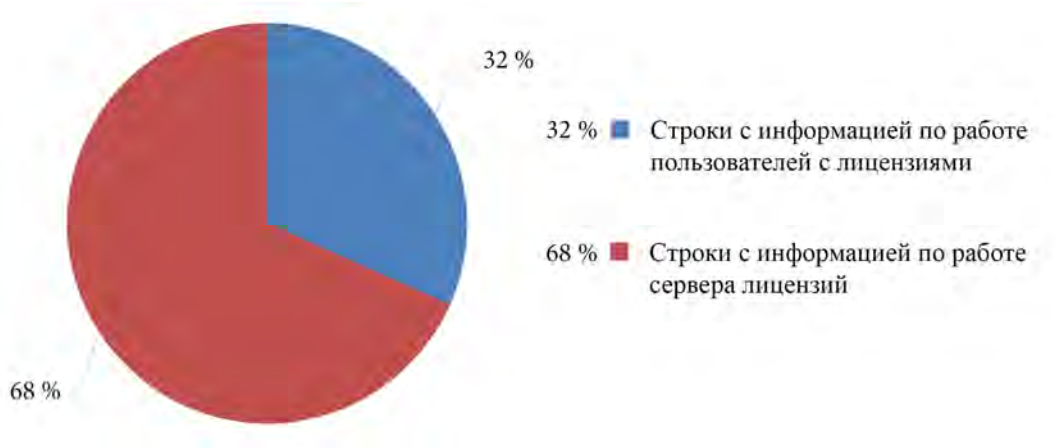


Рис. 2. Диаграмма распределения строк с информацией по работе пользователей и сервера лицензий в лог файле

что АКЛЗ на ПО направления 3D в СВС ВНИИЭФ представлены только двумя разработчиками Sentinel и Guardant.

Основной целью работы являлась реализация препроцессора для первичной обработки лог файлов АКЛЗ Sentinel и формирования статистических данных использования лицензий пользователями для задач, описанных во введении. В качестве побочных целей, достижение которых привело бы к более качественному обслуживанию ИС КП и ТПП являлись:

– уменьшение трудозатрат оператора при подготовке статистических отчётов;

– упрощение принятия решений в области управления лицензиями;

– уменьшение времени, затрачиваемого на принятие решений в области закупочной политики программного обеспечения.

Требуемая для отчетности и анализа статистическая информация, получаемая после обработки лог файлов АКЛЗ достаточно разнообразна:

– информация по определённому интервалу времени об использованном количестве тех или иных лицензий в разрезе учетных записей пользователей и программных продуктов;

– информация о времени использования лицензий в разрезе пользователей и программного продукта.

После анализа видов требующихся статистических данных, был сформирован ряд требований для выходных данных препроцессора.

Анализ лог файлов аппаратных ключей лицензионной защиты Sentinel

Лог файлы ключей Sentinel представляют собой структурированные файлы текстового формата с записями событий использования лицензий в хронологическом порядке. Строки лог файла ключей Sentinel условно можно разделить на два типа:

Первый тип – строки с информацией по работе пользователей с лицензиями. Они представляют собой текстовые строки, описывающие начало или окончание работы пользователя с какой-либо лицензией. В них содержится информация о дате и времени события, учётной записи пользователя, время длительности каждой сессии, уникальный модификатор сессии, идентификатор ключа HASP.

Второй тип – строки с информацией по работе сервера лицензий. Они представляют собой текстовые строки, описывающие начало или окончание работы сервера лицензий с какой-либо лицензией. В них содержится информация о дате и времени события, наименование сервера лицензий, время длительности каждой сессии, уникальный модификатор сессии, идентификатор ключа HASP.

Для определения стратегии разработки препроцессора был проведён анализ лог файлов на предмет выявления соотношения различных типов строк. Для разбора были взяты несколько случайных лог файлов, в каждом из которых подсчитывалось количество различных типов строк. В итоге было найдено среднее арифметическое значений по каждому типу строк, представленное на рис. 7.

ЭВМ, где размещены аппаратные ключи лицензионной защиты Sentinel, настроена на разовую ежесуточную аппаратную перезагрузку в момент гарантированного отсутствия пользователей на рабочих местах (00:00), в следствии чего сервер лицензирования создаёт новый лог файл, именованный по дате своего создания. В результате данных настроек информация по работе сервера лицензирования и пользователей записывается в отдельный лог файл, рис. 2. При интенсивной и/или длительной работе большого числа пользователей с программными продуктами в лог файлах накапливается большое количество записей, что значительно усложняет их анализ.

Структура строки, содержащей информацию о выдаче лицензии пользователю, представлена на рис. 3.

Структура строки, содержащей информацию о возвращении лицензии, ранее выданной пользователю, представлена на рис. 4.

Структура строки, содержащей информацию о начале работы сервера лицензий с программным продуктом, представлена на рис. 5.

Структура строки, содержащей информацию о завершении работы сервера лицензий с программным продуктом, представлена на рис. 6.

В своей работе препроцессор использует данные, взятые из строк с информацией по работе пользователей с лицензиями. Строки с информацией по работе сервера лицензий несут избыточные данные для препроцессора.

Разработка препроцессора

Входными данными препроцессора являются необработанные лог файлы ключей аппаратной защиты Sentinel. Как было описано выше в каждом лог файле есть типы строк, описывающие работу сервера лицензий, которые не несут в себе информации о работе пользователей с программными продуктами, следовательно, препроцессор не должен тратить время на их обработку. Строки, содержащие информацию о работе пользователей с лицензиями, содержат в себе ключевые наборы символов «LOGIN» и «LOGOUT». Таким образом, препроцессор при работе с лог файлом пропускает строки, не содержа-

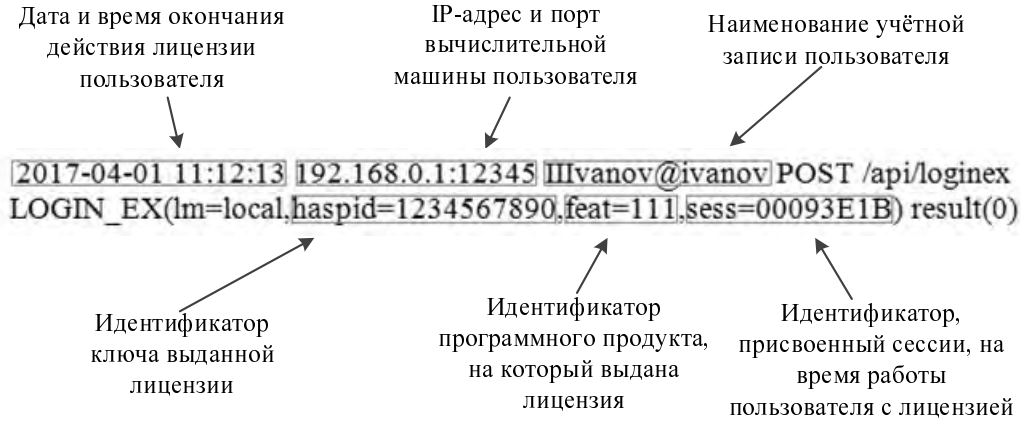


Рис. 3. Структура строки, содержащей информацию о выдаче лицензии пользователю

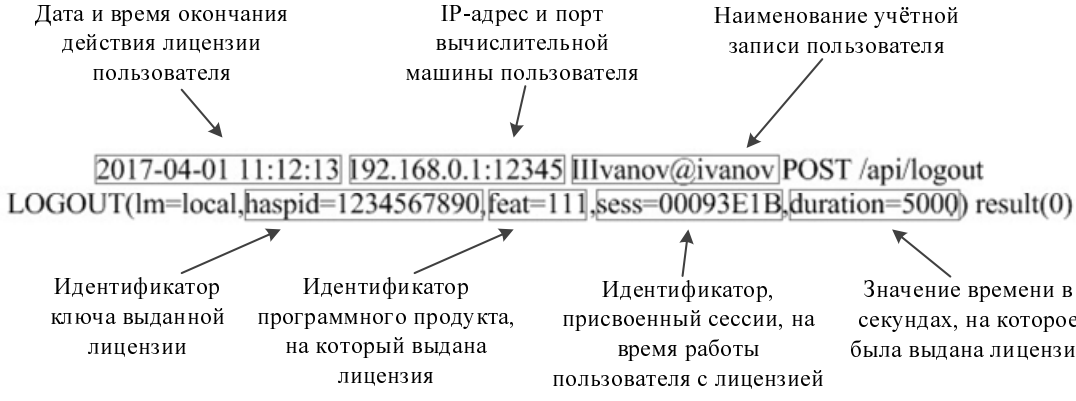


Рис. 4. Структура строки, содержащей информацию о возвращении лицензии, ранее выданной пользователю

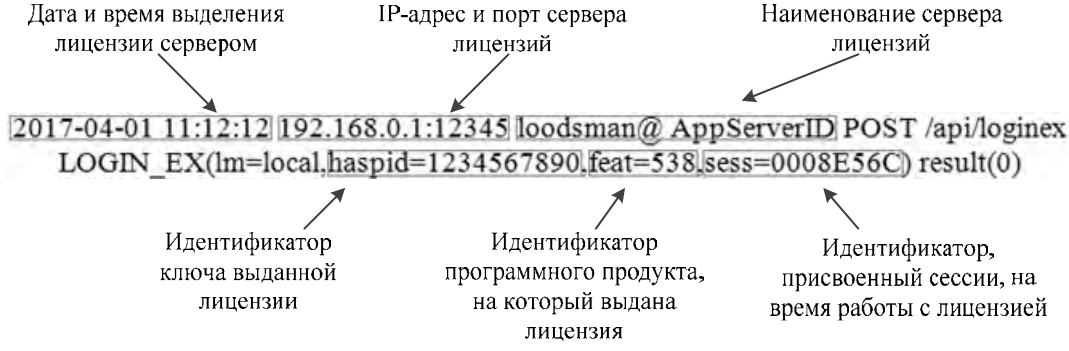


Рис. 5. Структура строки, содержащей информацию о начале работы сервера лицензий с программным продуктом

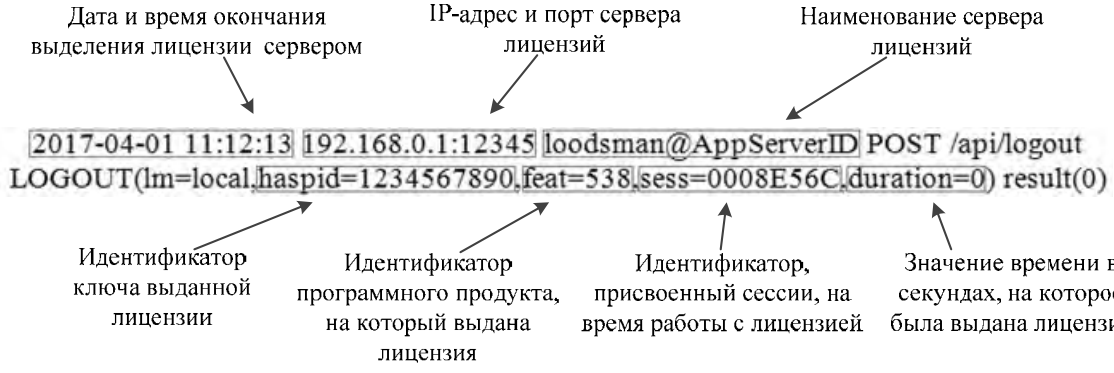


Рис. 6. Структура строки, содержащей информацию о завершении работы сервера лицензий с программным продуктом

щие в себе ключевые наборы символов, а строки, содержащие их, подвергаются дальнейшей обработке. Затем программа считывает необходимые последовательности символов из строк лог файла и передаёт их в массив для дальнейшей обработки.

Дальнейшая работа препроцессора различается, в зависимости от выбора режима работы. Эти режимы можно разделить на два типа:

– подготовка файлов данных по определённому интервалу времени о пиках использованных лицензий в разрезе учетных записей пользователей и программных продуктов;

– подготовка файлов данных о времени использования лицензий в разрезе учётных записей пользователей и программного продукта.

При дальнейшей работе препроцессора в первом режиме в массив поступают следующие данные:

– идентификатор лицензии,

– время начала сессии с лицензией и время конца сессии с лицензией.

Каждая строка лог файла, содержащая в себе информацию о работе пользователя с лицензией, порождает добавление в массив трёх новых значений. Число записей массива будет равно числу значимых строк в лог файле. После этого препроцессор подсчитывает сумму одновременно используемых лицензий в каждую секунду времени. Далее идёт построчное наполнение файла, где первая строка состоит из наименований программных продуктов, отделённых друг от друга разделителями. Следующие строки содержат значения даты и времени, после которых через разделители идёт количество активных лицензий в данный момент времени. В результате, выходными данными является структурированный текстовый файл формата csv, название которого совпадает с названием обработанного лог файла.

При дальнейшей работе препроцессора во втором режиме в массив поступают следующие данные:

– идентификатор лицензии,

– наименование учётной записи пользователя,

– время начала сессии с лицензией и время конца сессии с лицензией.

Каждая строка лог файла, содержащая в себе информацию о работе пользователя с лицензией, порождает добавление в массив четырёх новых значений. Далее препроцессор считывает наименования всех учётных записей пользователей и, выполняя проверку их уникальности, вносит в массив. Затем для каждой уникальной учётной записи выполняется суммирование времени работы пользователя с каждой лицензией. Далее идёт построчное наполнение файла, где первая строка состоит из наименований программных продуктов, отделённых друг от друга разделителями. Следующие строки содержат наименования учётных записей пользователей, после которых через разделители идёт общее время работы пользователя с определённым программным продуктом.

Выходные данные при работе препроцессора в первом режиме: файлы текстового формата с разделителями для удобного и быстрого импорта в Excel и последующей обработки. Возможный вид выходного файла данных при работе препроцессора в первом режиме представлен на рис. 7.

Выходные данные при работе препроцессора во втором режиме: файлы текстового формата с разделителями для удобного и быстрого импорта в Excel и последующей обработки. Возможный вид выходного файла данных при работе препроцессора во втором режиме представлен на рис. 8.

Для упрощения работы пользователей с препроцессором был сделан специальный графический интерфейс. Возможный вид окна графического интерфейса представлен на рис. 9.

Реализована возможность пакетной подачи файлов на обработку. Так как один лог файл описывает один день работы сервера лицензий, необходима возможность обработки группы файлов. Таким образом, если выбрать вместо входного файла целый каталог, препроцессор обработает каждый лог файл в каталоге по порядку. После обработки каждого файла, создает соответствующий файл статистических данных.

В лог файлах наименования всех программных продуктов заменены на уникальные цифровые идентификаторы, в файлы статистики вместо наименова-

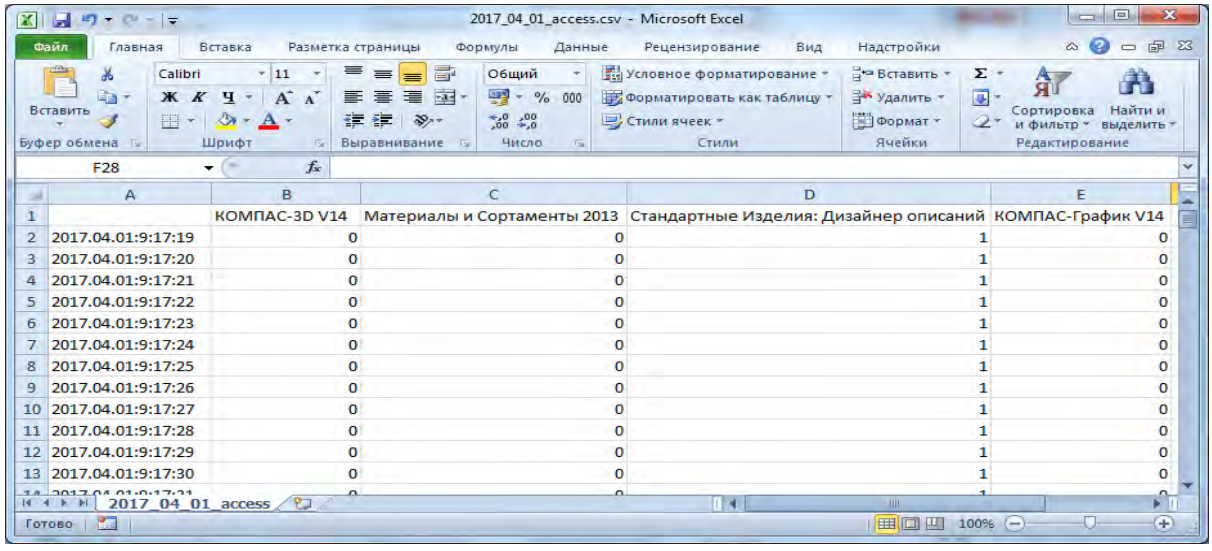


Рис. 7. Возможный вид выходного файла данных при работе препроцессора в первом режиме

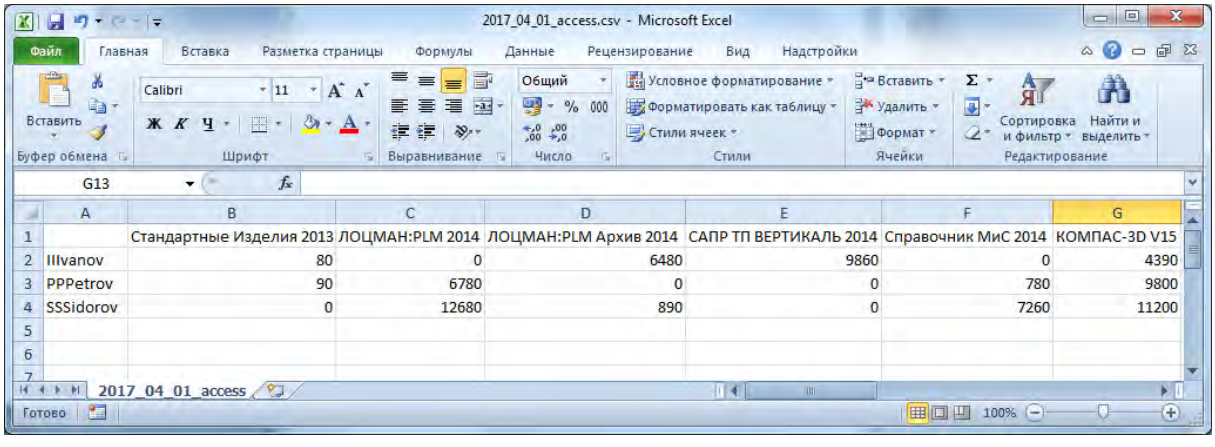


Рис. 8. Возможный вид выходного файла данных при работе препроцессора во втором режиме

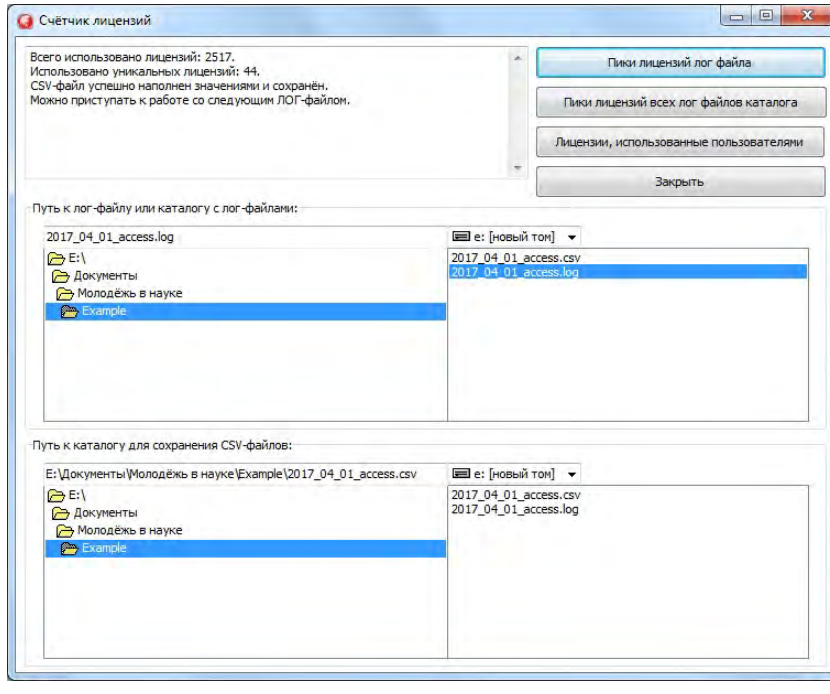


Рис. 9. Возможный вид окна препроцессора

ний передаются идентификаторы. Однако идентификаторы, представляющие собой числа неинформативны, поэтому целесообразно заменять их на наименования программных продуктов. При установке комплекса решений «АСКОН» создаётся отдельный XML файл, в котором идентификаторы продуктов сопоставлены с их наименованиями. Поэтому был создан специальный файл «словарь» в который вносятся значения идентификаторов продуктов, каждому из которых ставится в соответствие наименование продукта. При составлении выходного текстового файла с разделителями, препроцессор заменяет значения идентификаторов продуктов на соответствующие наименования из словаря.

При работе большого количества пользователей с программными продуктами в лог файлах накапливается большой объём информации, процесс обработки лог файлов может занимать довольно длительное время. Чтобы у оператора в любой момент времени была возможность прервать работу препроцессора, реализована возможность принудительной остановки работы приложения.

Заключение

В результате проделанной работы произведен поиск готовых решений по обработке лог файлов АКЛЗ и анализ средств лицензионной защиты ПО направления 3D, используемого в СВС ВНИИЭФ.

Разработано программное обеспечение – препроцессор, обладающий минимальным необходимым функционалом для получения статистической информации из лог файлов аппаратных ключей лицензионной защиты Sentinel, использующихся пользователями ПО «АСКОН». Графический интерфейс и функциональные возможности препроцессора, несомненно, будут развиваться в соответствии с поставленными аналитическими задачами по анализу деятельности пользователей в СВС ВНИИЭФ. Уже сейчас, разработанный препроцессор является мощным инструментом предоставления статистических данных полученных после обработки лог файлов АКЛЗ и открывает большие возможности для анализа и аналитики зон охвата лицензионным ПО рабочих мест пользователей и активности пользователей при проектировании на этапах внедрения больших ИС в масштабах предприятия.

Функционал работы с лог файлами АКЛЗ отличными от Sentinel будет добавлен в препроцессор в ближайшее время.

Литература

1. Скляров Д. В. Аппаратные ключи защиты // Искусство защиты и взлома информации. Санкт-Петербург «БХВ-Петербург», 2004. С. 288.

2. Юрасов А. В. Основы электронной коммерции. Горячая линия-Телеком, 2008. С. 480.

3. https://safenet.gemalto.com

4. https://www.guardant.ru