

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00077-06-ЛУ

«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4
АВТОМАТИЗИРОВАННЫЙ КЛИЕНТ СКЗИ
Руководство пользователя

ВАМБ.00077-06 92 03

2020

Аннотация

Данный документ содержит описание эксплуатации программного комплекса (ПК) ВАМБ.00077-06 12 02 «Автоматизированный клиент СКЗИ» (далее — ПК «АК СКЗИ»), входящего в состав ПК ВАМБ.00077-06 «“Валидата Клиент” версия 4» (далее — ПК «Валидата Клиент»).

Документ предназначен для пользователей как руководство по эксплуатации ПК «АК СКЗИ».

Перед чтением настоящего руководства следует ознакомиться с документом ВАМБ.00077-06 31 01 «“Валидата Клиент” версия 4. Описание применения».

Содержание

1 НАЗНАЧЕНИЕ, СОСТАВ И ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ	5
1.1 Назначение ПК «АК СКЗИ»	5
1.2 Требования к аппаратно-программной среде	5
1.3 Состав ПК «АК СКЗИ»	5
2 ЗАПУСК ПК «АК СКЗИ»	6
2.1 Процедура запуска ПК «АК СКЗИ»	6
2.2 Первый запуск ПК «АК СКЗИ»	6
3 РАБОТА С ПК «АК СКЗИ»	7
3.1 Интерфейс и структура модуля конфигурации ПК «АК СКЗИ»	7
3.2 Общие настройки ПК «АК СКЗИ»	7
3.3 Работа с профилями ПК «АК СКЗИ»	11
3.3.1 Создание профиля ПК «АК СКЗИ»	11
3.3.2 Настройки профиля ПК «АК СКЗИ»	11
3.3.3 Переключение профилей ПК «АК СКЗИ»	17
3.3.4 Редактирование профиля ПК «АК СКЗИ»	18
3.3.5 Удаление профиля ПК «АК СКЗИ»	19
3.4 Работа с правилами профиля ПК «АК СКЗИ»	20
3.4.1 Создание правила	20
3.4.2 Работа с масками	23
3.4.3 Работа с сертификатами получателей	25
3.4.4 Работа с параметрами операции «Переместить»	30
3.4.5 Настройка архивации правил	31
3.4.6 Настройка типа операции подписания	32
3.4.7 Работа с параметрами операции «Переподписать»	33
3.4.8 Работа с параметрами операции «Упаковать файлы»	33
3.4.9 Работа с параметрами операции «Исполнить»	34
3.4.10 Работа со списками подписантов	35
3.4.11 Описание правил	40
3.4.12 Копирование правил	40
3.4.13 Редактирование правил	41
3.4.14 Удаление правил	41
3.4.15 Изменение порядка исполнения правил	42
3.4.16 Временное отключение правил	42
3.4.17 Отображение информации о пункте правила	43
3.4.18 Экспорт правил профиля	43
3.4.19 Импорт правил профиля	44
3.4.20 Поиск правил по описанию	44
3.5 Сохранение внесенных изменений	45
3.6 Выход из программы конфигурации	45
3.7 Интерфейс обработчика ПК «АК СКЗИ»	46
3.8 Запуск обработчика ПК «АК СКЗИ»	46
3.9 Остановка обработчика ПК «АК СКЗИ»	46

3.10 Обработка ошибок ПК «АК СКЗИ»	47
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	48
ПЕРЕЧЕНЬ РИСУНКОВ	49
ПЕРЕЧЕНЬ ТАБЛИЦ	51

1 НАЗНАЧЕНИЕ, СОСТАВ И ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ СРЕДЕ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

1.1 Назначение ПК «АК СКЗИ»

ПК «АК СКЗИ» предназначен для автоматизации работы пользователя с криптографическими функциями.

1.2 Требования к аппаратно-программной среде

Требования к аппаратно-программной среде, в которой функционирует ПК «АК СКЗИ», приведены в документе ВАМБ.00077-06 30 01 «“Валидата Клиент” версия 4. Формуляр».

1.3 Состав ПК «АК СКЗИ»

ПК «АК СКЗИ» из состава ПК «Валидата Клиент» реализован в виде конфигурационного модуля «АК СКЗИ - конфигурация.exe» и модуля-обработчика «АК СКЗИ - обработчик.exe».

Состав ПК «АК СКЗИ» приведен в документе ВАМБ.00077-06 91 02 «“Валидата Клиент” версия 4. Автоматизированный клиент СКЗИ. Руководство по установке и настройке».

2 ЗАПУСК ПК «АК СКЗИ»

2.1 Процедура запуска ПК «АК СКЗИ»

Конфигурационный модуль запускается из основного меню ОС Microsoft Windows **«Программы» – «ПК Валидата Клиент» – «АК СКЗИ - конфигурация»**. Обработчик ПК «АК СКЗИ» запускается из основного меню ОС Microsoft Windows **«Программы» – «ПК Валидата Клиент» – «АК СКЗИ - обработчик»**.

2.2 Первый запуск ПК «АК СКЗИ»

Для работы ПК «АК СКЗИ» требуется конфигурация, состоящая из профилей, содержащих правила обработки файлов. При первом запуске обработчика или модуля конфигурации будет автоматически создан стандартный профиль «default», не содержащий правил. Для создания новых профилей и добавления в них правил необходимо воспользоваться конфигурационным модулем «АК СКЗИ - конфигурация».

Внимание: внесение изменений в конфигурацию ПК «АК СКЗИ» происходит при сохранении изменений в конфигурационном модуле. Для того чтобы изменения в конфигурации вступили в силу для уже работающего профиля ПК «АК СКЗИ», этот профиль необходимо перезапустить.

3 РАБОТА С ПК «АК СКЗИ»

3.1 Интерфейс и структура модуля конфигурации ПК «АК СКЗИ»

Графический интерфейс и структура модуля конфигурации ПК «АК СКЗИ» приведены на рисунке (Рисунок 1).

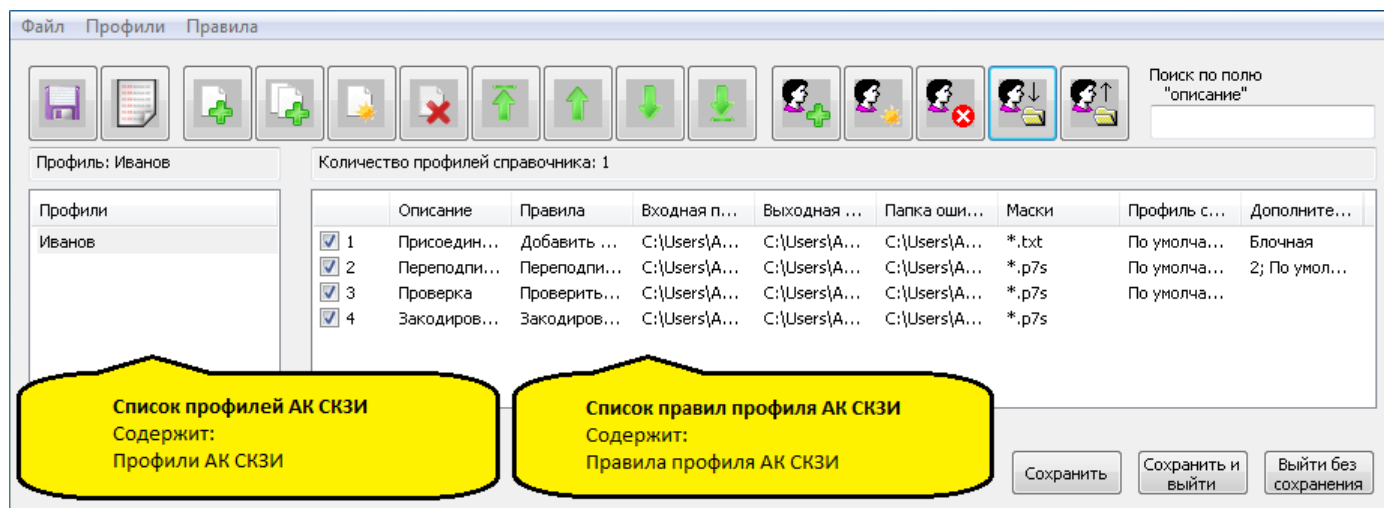


Рисунок 1 – Интерфейс модуля конфигурации ПК «АК СКЗИ»

3.2 Общие настройки ПК «АК СКЗИ»

Для настройки конфигурации ПК «АК СКЗИ» необходимо выполнить следующие действия:

- выбрать путь для записи журнала (по умолчанию запись идет в папку C:\Users*Пользователь*\AppData\Roaming\Validata\zpkitrays);
- настроить расширения для обрабатываемых файлов;
- настроить профиль по умолчанию «default» или создать новый;
- создать правила обработки файлов в выбранном профиле.

Выбор пути записи журнала выполняется нажатием кнопки «Путь журнала» (Рисунок 2).

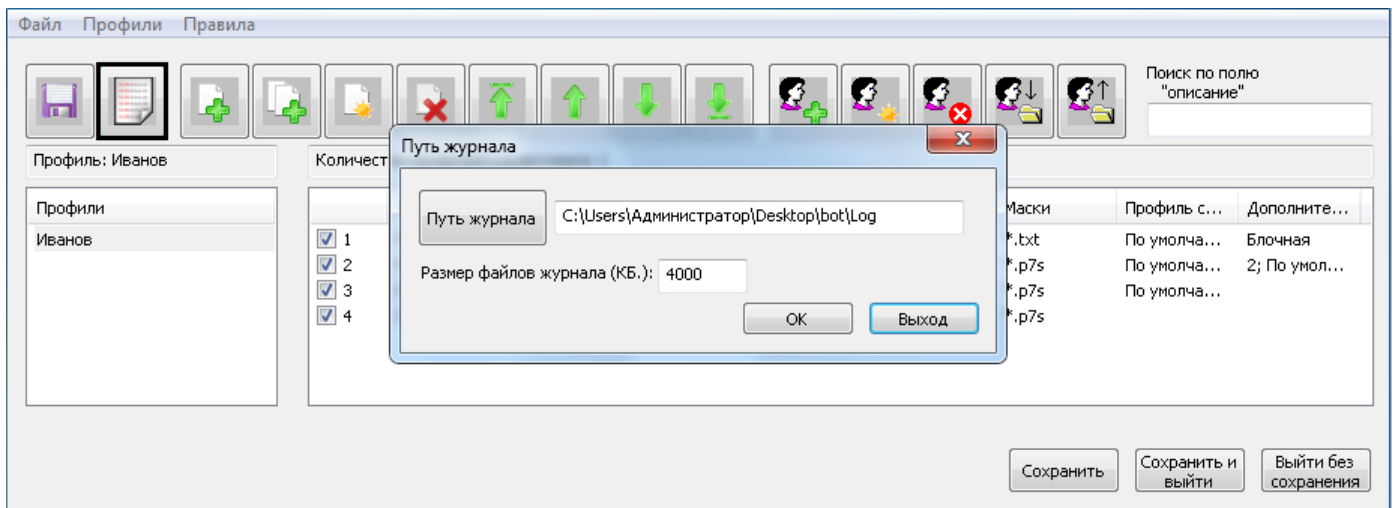


Рисунок 2 – Выбор пути записи журнала

Путь журнала можно выбрать с помощью кнопки «Путь журнала» или ввести вручную. После ввода пути программа проведет его проверку.

Журнал ПК «АК СКЗИ» разбивается на файлы, размер которых задается с помощью поля «Размер файлов журнала». По умолчанию размер файлов составляет 4000 килобайт и не может быть установлен меньше 400 килобайт.

При возникновении повторяющейся ошибки доступа к одной из папок, используемых в правилах, запись в журнал об ошибке будет добавляться раз в час, чтобы избежать переполнения журнала.

Настройка расширений для обрабатываемых файлов производится из меню «Настройки», вызываемого нажатием кнопки «Настройки» в меню «Файл» (Рисунок 3).

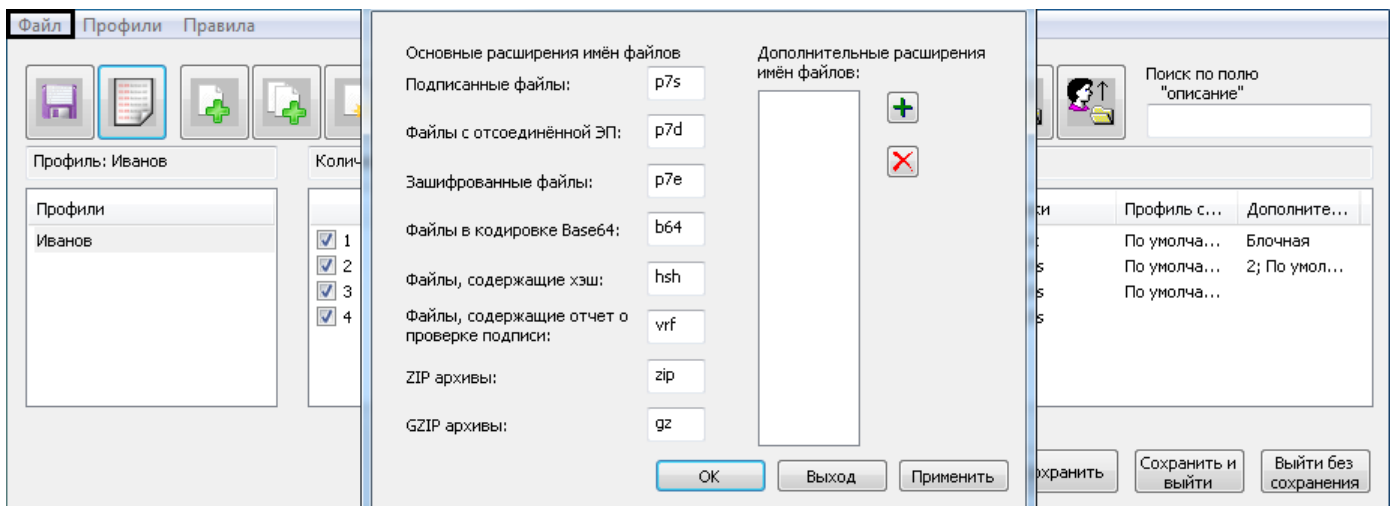


Рисунок 3 – Настройка расширений для обрабатываемых файлов

Таблица 1 – Настройки расширений для обрабатываемых файлов

Название параметра	Описание	Значение по умолчанию (после установки)
Подписанные файлы	Расширение, которое добавляется к файлу при создании присоединённой ЭП и снимается при удалении ЭП.	p7s
Файлы с отсоединённой ЭП	Расширение, которое добавляется к файлу при создании отсоединённой ЭП.	p7d
Зашифрованные файлы	Расширение, которое добавляется к файлу при зашифровании и снимается при расшифровании.	p7e
Файлы в кодировке Base64	Расширение, которое добавляется к файлу при преобразовании в кодировку Base64 и снимается при преобразовании из кодировки Base64.	b64
Файлы, содержащие хэш	Расширение, которое добавляется к файлу, содержащему хэш.	hsh
Файлы, содержащие отчет о проверке подписи	Расширение, которое добавляется к файлу, содержащему отчет о проверке подписи после успешной проверки подписи файла.	vrf
ZIP архивы	Расширение, добавляемое к файлам при использовании ZIP архивации и удаляемое при разархивации ZIP архивов.	zip
GZIP архивы	Расширение, добавляемое к файлам при использовании GZIP архивации и удаляемое при разархивации GZIP архивов.	gz
Дополнительные расширения имён файлов	Список расширений, которые снимаются с файлов при удалении ЭП и расшифровании.	Пустой список

Расширения имён файлов определяют, с каким расширением будут создаваться файлы в результате операций (например, файлы «*.p7s» как результат функции «Добавить присоединенную подпись»), а также как программа будет воспринимать входящие файлы (например, файлы с расширением «*.p7s» для функции «Добавить присоединенную подпись» будут восприниматься как файлы, содержащие присоединенную подпись, и их расширение в результате функции не будет изменяться).

Существует возможность добавлять дополнительные расширения с помощью кнопки «Добавить расширение» (Рисунок 4).

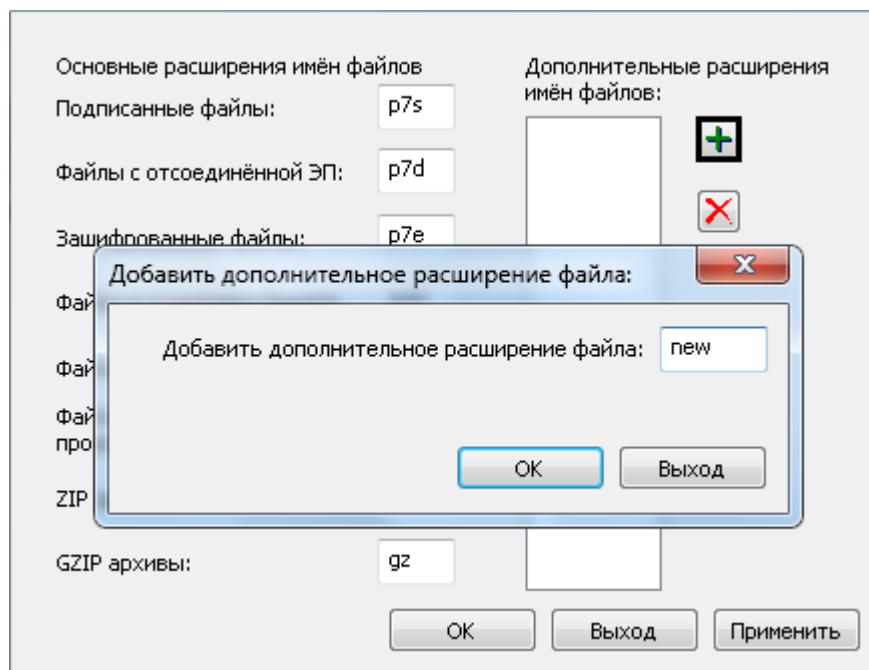


Рисунок 4 - Добавление дополнительного расширения

Для удаления дополнительных расширений необходимо выбрать расширение в списке дополнительных расширений и нажать кнопку «Удалить расширение» (Рисунок 5).

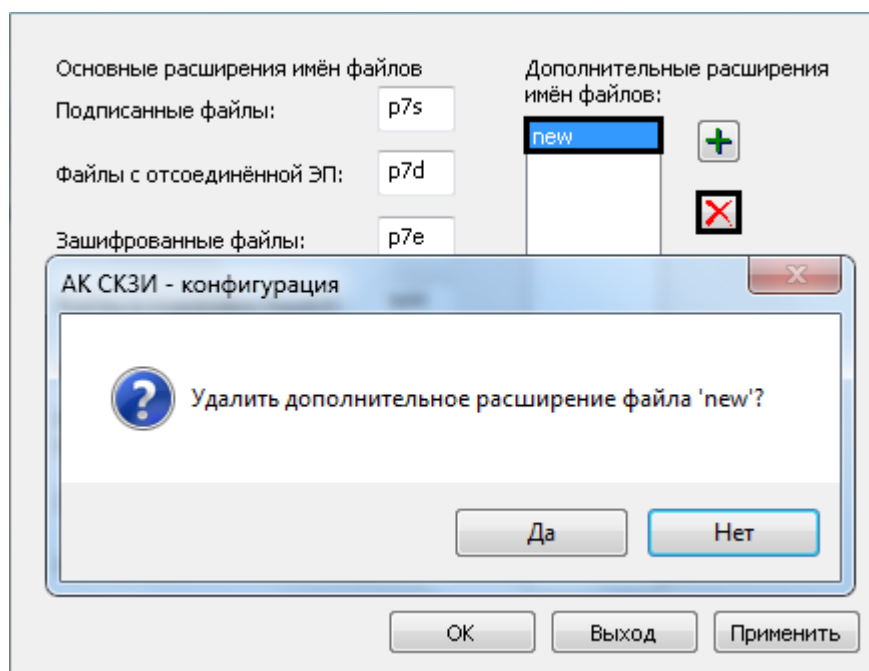


Рисунок 5 - Удаление дополнительного расширения

Начиная обработку файла, программа переименовывает его, добавляя специальное расширение ztr. Файлы с таким расширением будут игнорироваться другими работающими профилями. Если во время обработки произошла критическая ошибка или к файлу невозможно было получить необходимый доступ,

файл остается со специальным расширением, пока его не переименуют вручную. В случае конфликта имен при попытке переименовать файл в расширение ztr файл будет пропускаться.

3.3 Работа с профилями ПК «АК СКЗИ»

3.3.1 Создание профиля ПК «АК СКЗИ»

Создание нового профиля выполняется нажатием кнопки «Добавить профиль» (Рисунок 6).

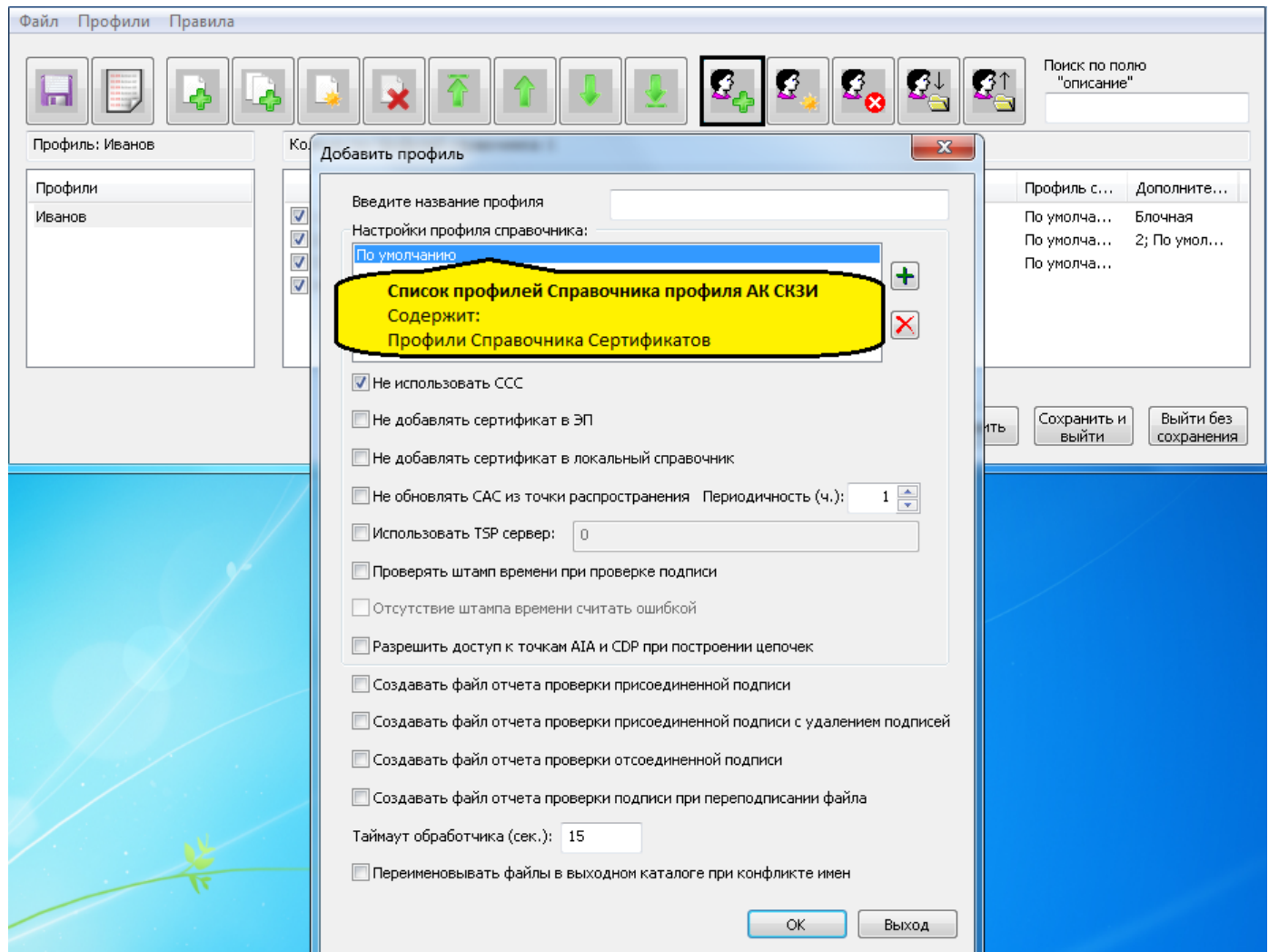


Рисунок 6 – Создание нового профиля

Необходимо указать имя профиля (имя профиля должно быть уникально, не может быть пустым) и выбрать необходимые настройки.

3.3.2 Настройки профиля ПК «АК СКЗИ»

Окно создания нового профиля содержит список профилей справочника, с которыми будет работать создаваемый профиль ПК «АК СКЗИ». Выбранные профили можно будет использовать при создании правил.

Новые профили справочника добавляются кнопкой «Добавить профиль справочника» (Рисунок 7).

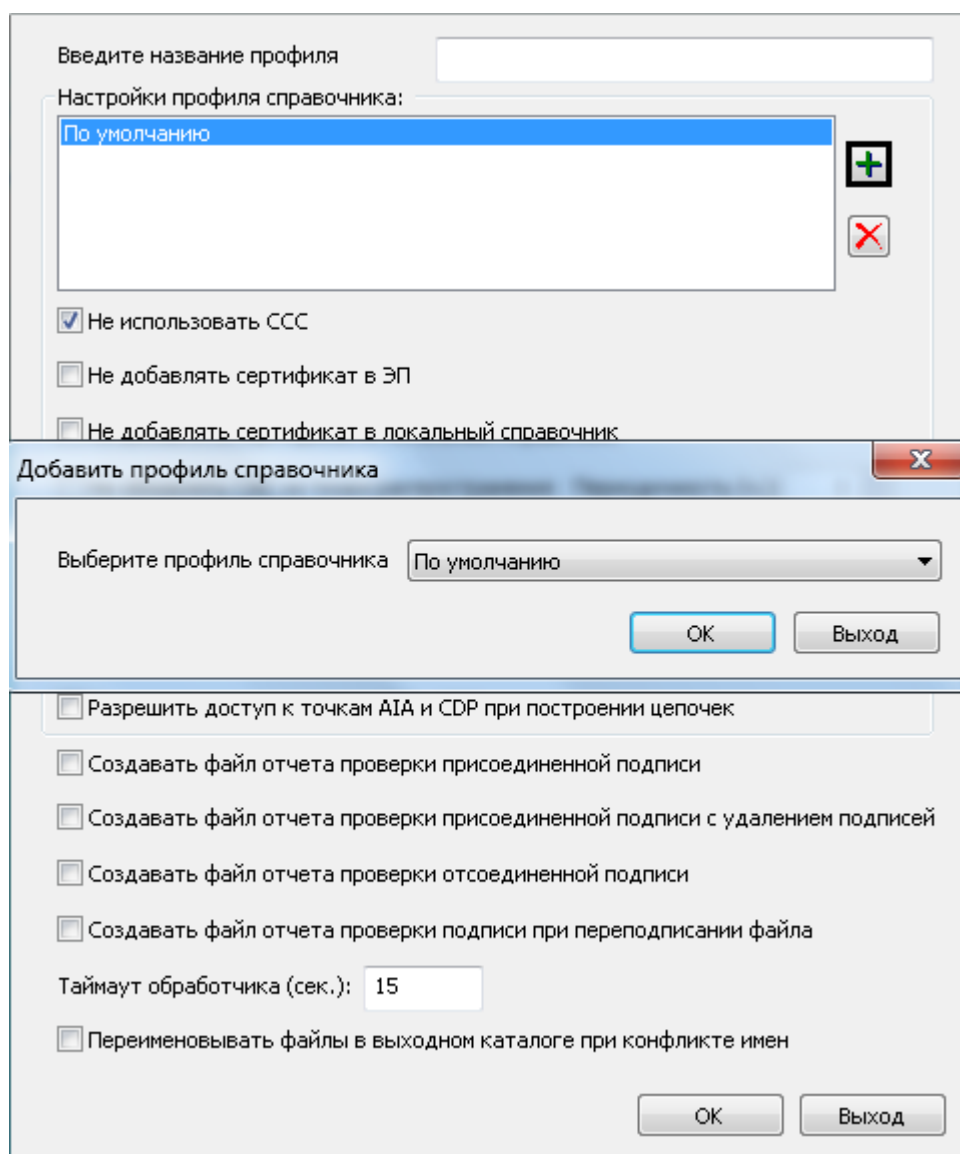


Рисунок 7 – Добавление профиля справочника в список

Для добавления профиля справочника необходимо выбрать нужный профиль из списка профилей справочника и нажать кнопку «ОК» (Рисунок 8).

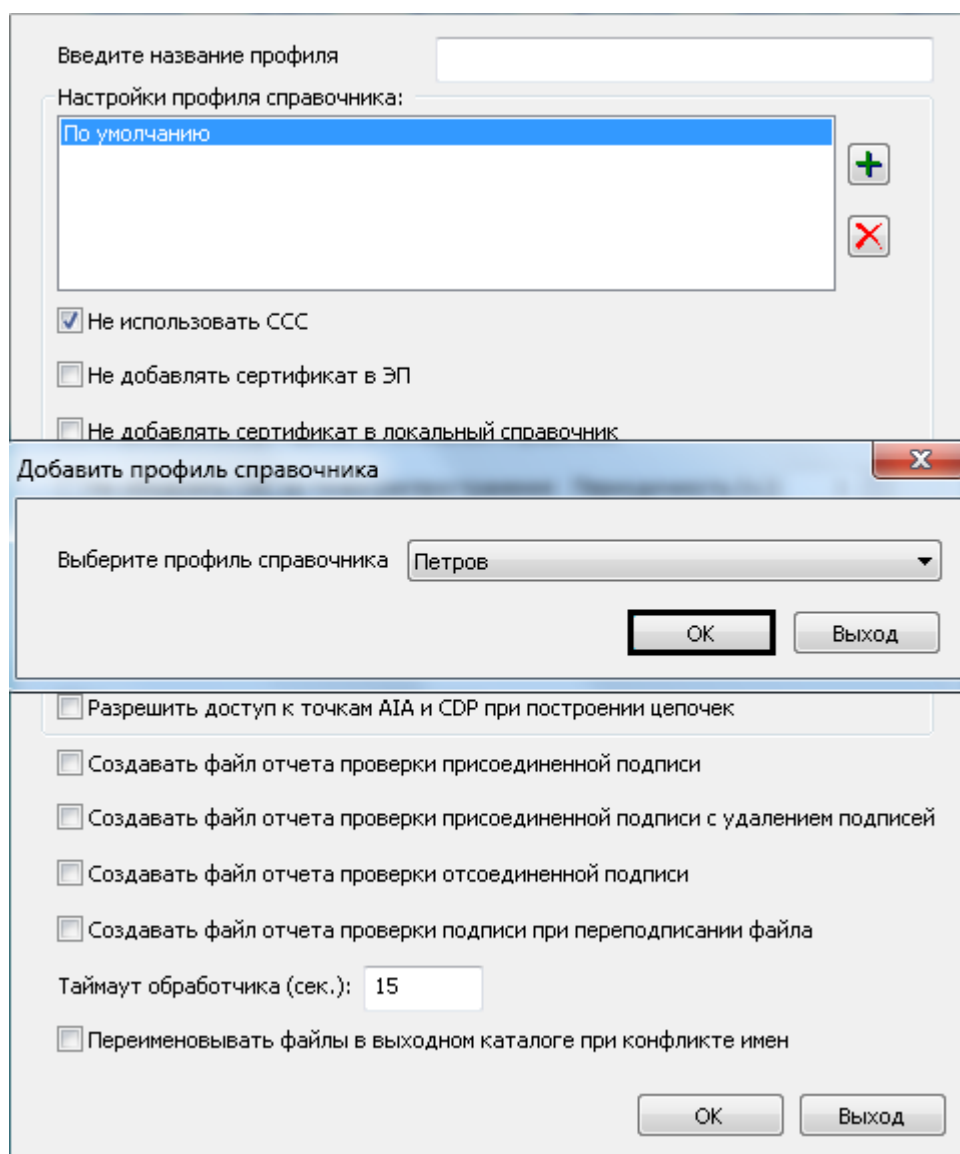


Рисунок 8 – Выбор профиля из списка профилей справочника

Для каждого профиля справочника в профиле ПК «АК СКЗИ» есть ряд индивидуальных настроек. Переключение между настройками профилей справочника производится путем выбора необходимого профиля в списке профилей справочника (Рисунок 9).

Введите название профиля

Настройки профиля справочника: Петров

По умолчанию
Петров

☒ Не использовать CCC

☒ Не добавлять сертификат в ЭП

☒ Не добавлять сертификат в локальный справочник

☒ Не обновлять САС из точки распространения Периодичность (ч.):

☐ Использовать TSP сервер:

☐ Проверять штамп времени при проверке подписи

☐ Отсутствие штампа времени считать ошибкой

☐ Разрешить доступ к точкам AIA и CDP при построении цепочек

☐ Создавать файл отчета проверки присоединенной подписи

☐ Создавать файл отчета проверки присоединенной подписи с удалением подписей

☐ Создавать файл отчета проверки отсоединенной подписи

☐ Создавать файл отчета проверки подписи при переподписании файла

Таймаут обработчика (сек.):

☐ Переименовывать файлы в выходном каталоге при конфликте имен

OK Выход

Рисунок 9 - Переключение между настройками профилей справочников

Таблица 2 - Настройки профиля, привязанные к выбранному профилю справочника

Название параметра	Описание	Значение по умолчанию (после установки)
Не использовать LDAP	Отключить использование сетевого справочника, указанного в настройках Справочника сертификатов, при операциях проверки подписи и поиска сертификатов для зашифрования	Выключено
Не добавлять сертификат в ЭП	Отключить режим включения в ЭП сертификата, на котором создаётся ЭП	Выключено
Не добавлять сертификат в локальный справочник	Отключить режим добавления сертификата, найденного в сетевом справочнике в базу сертификатов Справочника сертификатов. (Изменения вступают в силу после загрузки ключа)	Выключено
Не обновлять САС из точки распространения	Отключить режим обязательного обновления САС из точки распространения при инициализации криптоконтекста (загрузке ключа). Обновление производится только если со времени предыдущего обновления прошло больше времени, чем указано в параметре "Периодичность"	Выключено
Периодичность (ч.)	Периодичность обновления САС	1 час
Использовать TSP сервер (выключатель)	При создании подписи добавлять в неё штамп времени с сервера, адрес которого задаётся следующим параметром	Выключено
Использовать TSP сервер (строка ввода)	Адрес TSP сервера, доступен для редактирования только при включённом предыдущем параметре	Пустая строка
Проверять штамп времени при проверке подписи	При проверке каждой подписи пытаться проверить для неё штамп времени. Ошибка проверки штампа времени считается ошибкой проверки подписи	Выключено
Отсутствие штампа времени считать ошибкой	Требовать наличие штампа времени. Отсутствие штампа времени хотя бы одной из подписей считается ошибкой проверки подписи. Доступен для изменения только при включённом предыдущем параметре	Выключено
Разрешить доступ к точкам AIA и CDP при построении цепочек	Разрешать доступ к точкам распространения сертификатов и САС при построении цепочек проверки сертификатов	Выключено

Таблица 3 – Общие настройки профиля ПК «АК СКЗИ»

Название параметра	Описание	Значение по умолчанию (после установки)
Название профиля	Позволяет ввести имя профиля	Пустая строка
Создавать файл отчета проверки присоединенной подписи	При успешной проверке подписей в выходном каталоге будет создаваться файл, содержащий информацию о проверенных присоединенных подписях	Выключено
Создавать файл отчета проверки присоединенной подписи с удалением подписей	При успешной проверке подписей в выходном каталоге будет создаваться файл, содержащий информацию о проверенных присоединенных и удаленных подписях	Выключено
Создавать файл отчета проверки отсоединенной подписи	При успешной проверке подписей в выходном каталоге будет создаваться файл, содержащий информацию о проверенных отсоединенных подписях	Выключено
Создавать файл отчета проверки подписи при переподписании файла	При успешной проверке подписей в выходном каталоге будет создаваться файл, содержащий информацию о проверенных присоединенных подписях переподписываемого файла	Выключено
Таймаут обработчика (сек.)	Значение, задающее время таймаута обработчика в секундах	15 секунд
Переименовывать файлы в выходном каталоге при конфликте имен	При возникновении конфликта имен в выходном каталоге в результате выполнения функции файл не будет отправляться в каталог, содержащий ошибки, а будет переименован с добавлением случайного числа в формате «имя число.расширение»	Выключено

Для удаления профиля из списка профилей справочника необходимо выбрать профиль в списке и нажать кнопку «Удалить профиль справочника» (Рисунок 10).

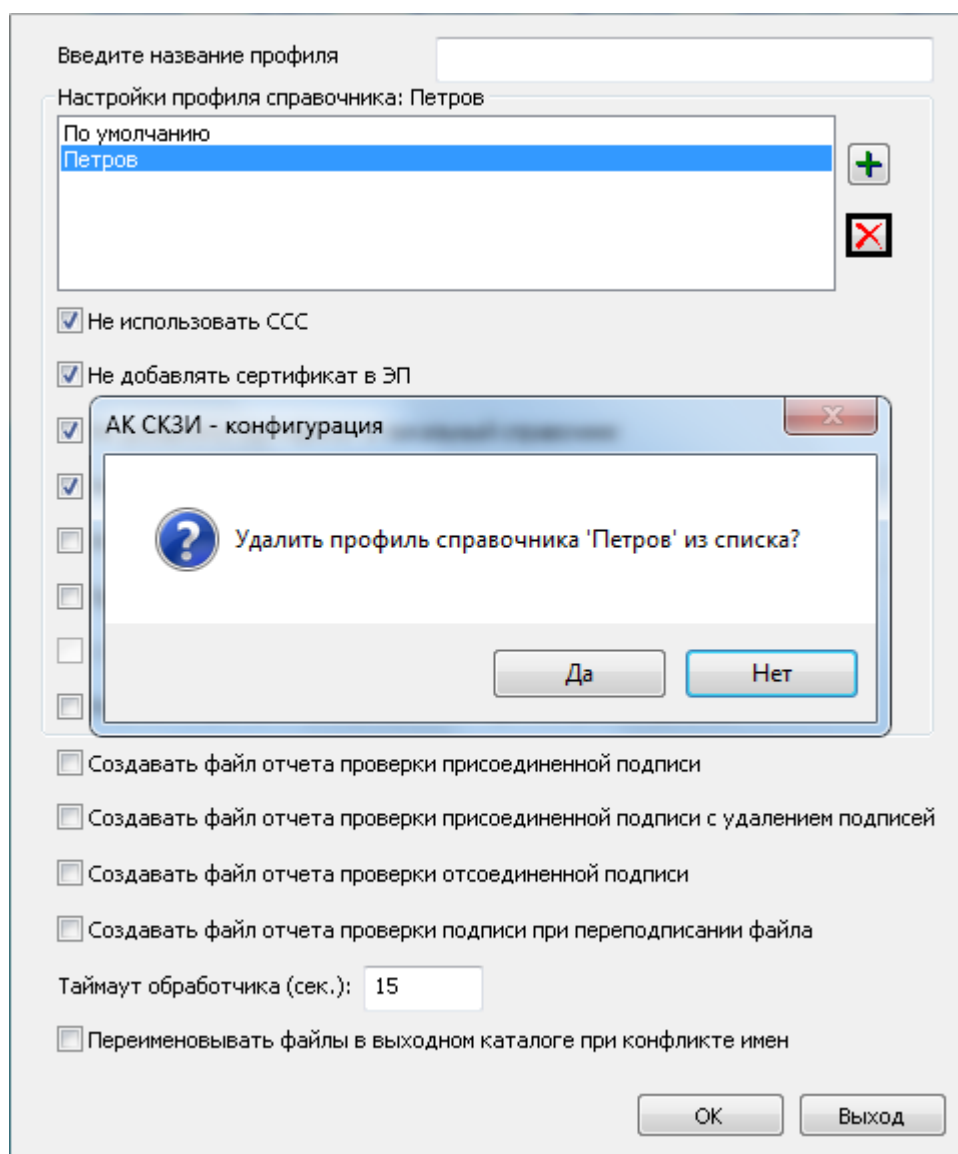


Рисунок 10 – Удаление профиля справочника из списка

Внимание: если в правилах редактируемого профиля (например, шифрование, проверка подписей или переподписание) использовались сертификаты удаляемого профиля справочника, для корректной работы этих правил после удаления профиля справочника их необходимо будет отредактировать. Если в редактируемом профиле ПК «АК СКЗИ» присутствовали правила, использовавшие удаляемый профиль справочника для операций, то для этих операций в качестве профиля справочника будет задан первый в списке редактируемого профиля ПК «АК СКЗИ» профиль справочника.

3.3.3 Переключение профилей ПК «АК СКЗИ»

Для открытия и редактирования правил профиля необходимо выбрать профиль в списке профилей нажатием левой кнопки мыши на его имя в списке профилей (Рисунок 11).

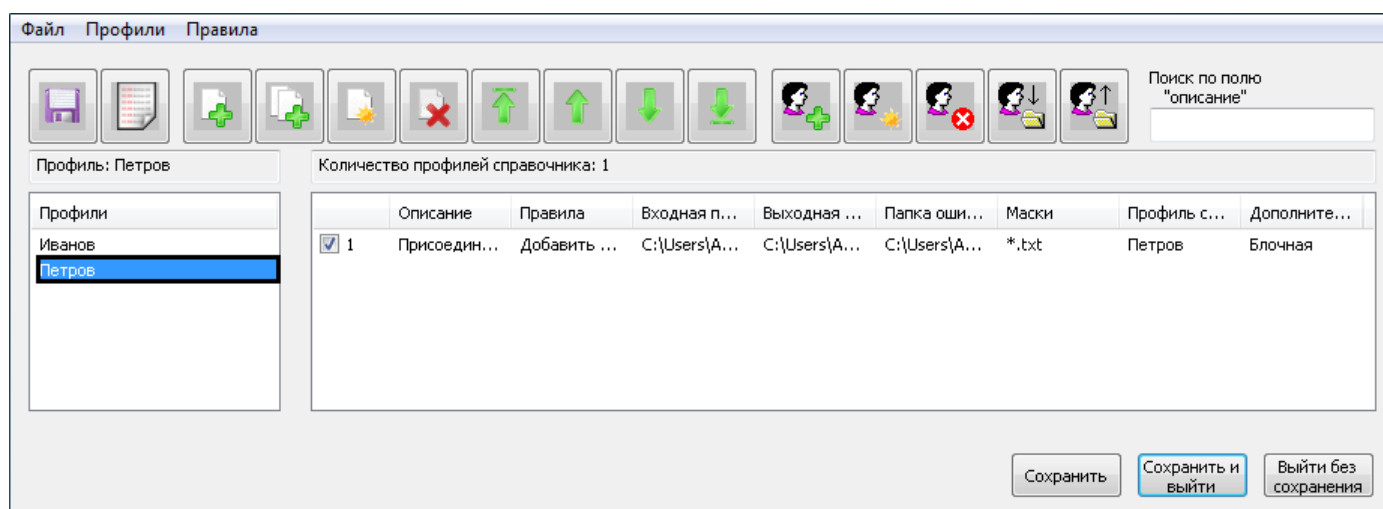


Рисунок 11 – Переключение профилей

После открытия профиля становятся доступны функции работы с профилем:

- «Редактировать профиль»;
- «Удалить профиль»;
- «Экспортировать профиль»;
- «Импортировать профиль»;

и функции работы с правилами:

- «Добавить правило»;
- «Редактировать правило»;
- «Удалить правило»;
- «Сделать правило первым»;
- «Сдвинуть правило вверх»;
- «Сдвинуть правило вниз»;
- «Сделать правило последним».

После удаления профиля перечисленные функции снова будут недоступны до открытия другого профиля из списка профилей.

3.3.4 Редактирование профиля ПК «АК СКЗИ»

Редактирование существующего профиля выполняется нажатием кнопки «Изменить профиль» или двойным кликом левой кнопкой мыши по имени профиля в списке (Рисунок 12).

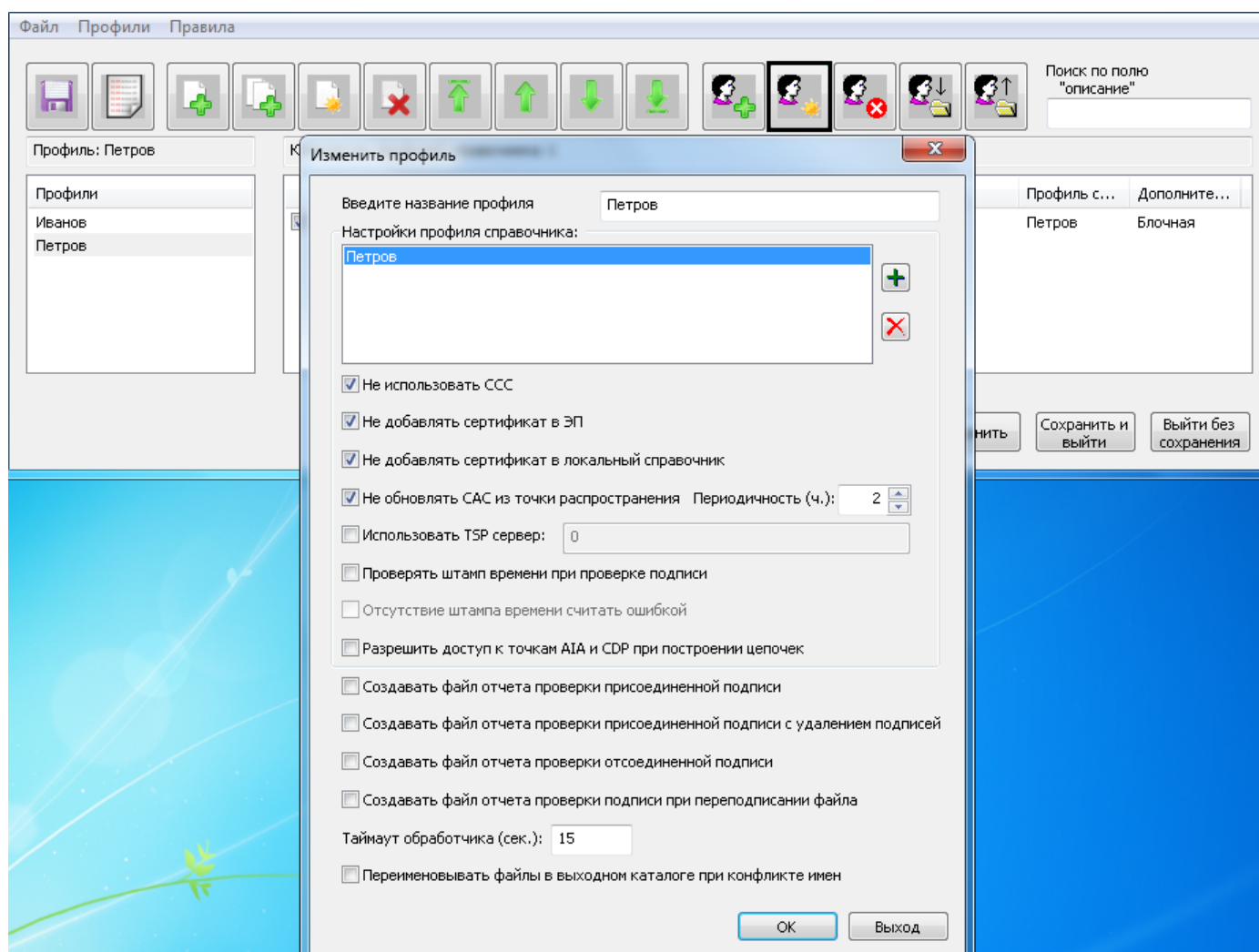


Рисунок 12 – Редактирование профиля

3.3.5 Удаление профиля ПК «АК СКЗИ»

Удаление текущего профиля выполняется нажатием кнопки «Удалить профиль» (Рисунок 13). Последний оставшийся профиль удалению не подлежит.

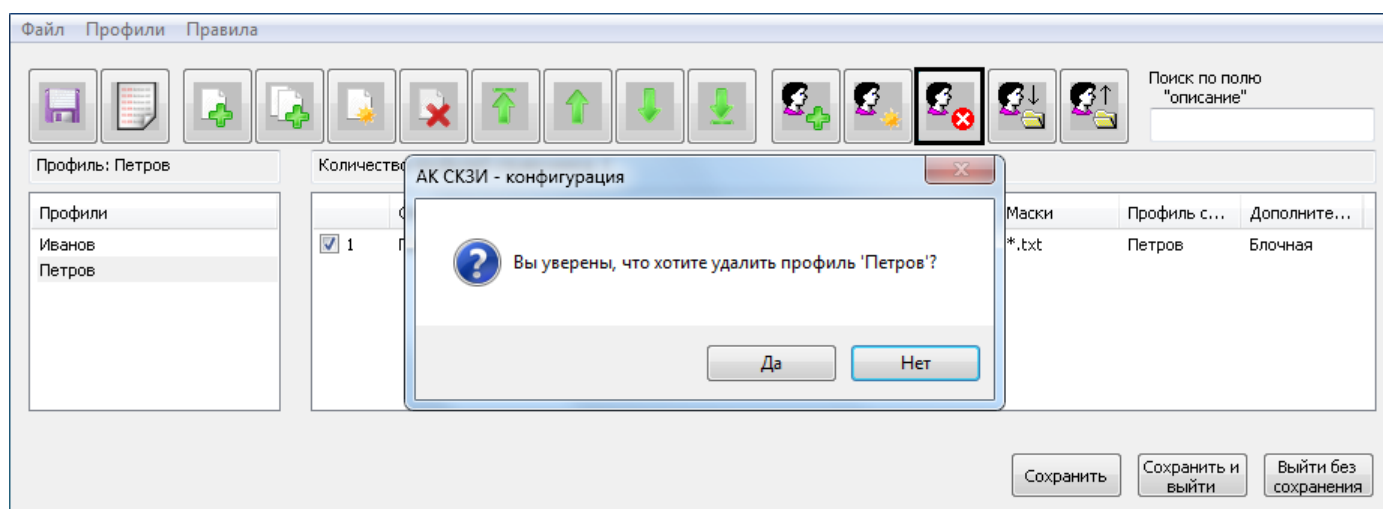


Рисунок 13 – Удаление профиля

3.4 Работа с правилами профиля ПК «АК СКЗИ»

3.4.1 Создание правила

Правила создаются нажатием кнопки «Добавить правило» и выбором необходимых параметров (Рисунок 14).

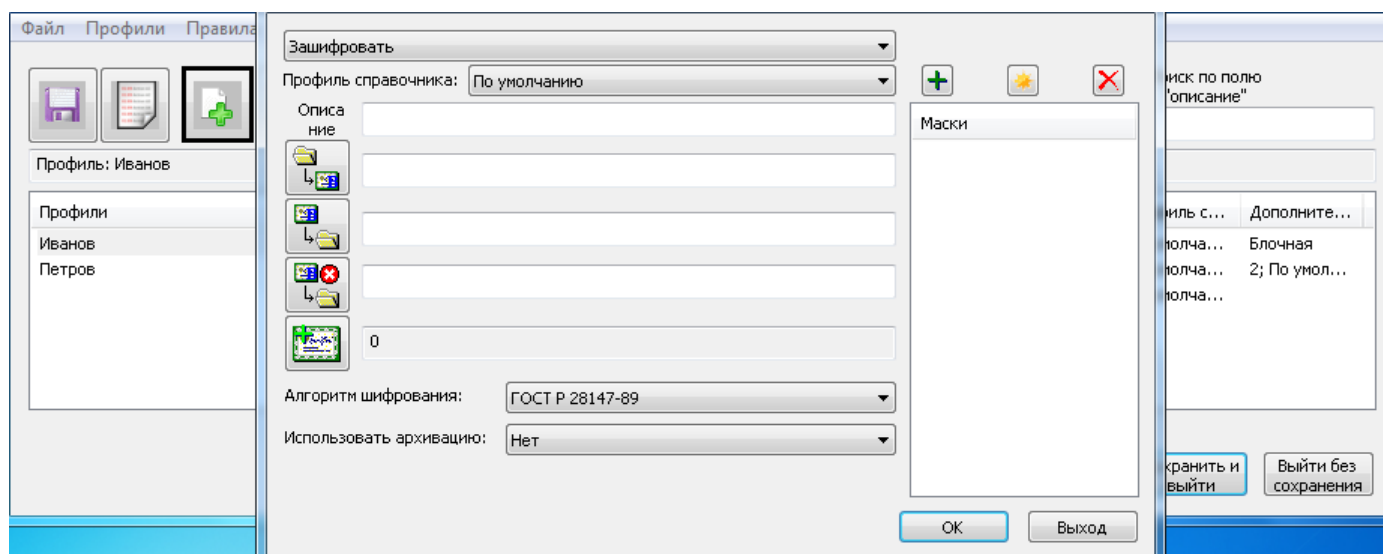


Рисунок 14 – Создание нового правила

Необходимо выбрать:

- тип операции;
- профиль Справочника Сертификатов с помощью выпадающего меню. Для операций «Удалить», «Переместить», «Закодировать в b64», «Раскодировать из b64», «Архивировать файл», «Разархивировать файл», «Упаковать файлы» и «Распаковать файлы» профили Справочника Сертификатов не используются;
- входную директорию, в которой будет выполняться поиск файлов по заданным маскам;

- выходную директорию, в которой будет размещаться результат операции в случае ее успеха. Не используется операцией «Удалить»;
- директорию, в которую отправляются файлы, при обработке которых произошла ошибка;
- список масок, по которым будет выполняться поиск файлов во входном каталоге;
- сертификаты получателей, для которых будет производиться шифрование, для операций «Зашифровать», «Зашифровать большой файл» и «Добавить присоединённую подпись и зашифровать»;
- алгоритм шифрования для операций «Зашифровать», «Зашифровать большой файл» и «Добавить присоединённую подпись и зашифровать»;
- тип создаваемой подписи для операций «Добавить присоединённую подпись» и «Добавить присоединённую подпись и зашифровать»;
- дополнительные параметры для операции «Переподписать».

Тип операции выбирается с помощью выпадающего меню из следующего списка:

1. Зашифровать: создает зашифрованный файл из исходного для заданного количества получателей. Максимальный размер файла ограничен разрядностью и размером оперативной памяти системы (примерно до 400 Мб для 32 разрядной системы и до 2 Гб для 64 разрядной). Для шифрования больших файлов рекомендуется использовать операцию «Зашифровать большой файл»;
2. Расшифровать: создает расшифрованный исходный файл из зашифрованного. Ограничение максимального размера соответствует ограничению операции «Зашифровать». Для расшифровки больших файлов используйте функцию «Расшифровать большой файл»;
3. Хэшировать файл: создает текстовый файл, содержащий три формата хэша исходного файла. В случае успеха исходный файл перемещается в выходной каталог;
4. Закодировать в b64: создает файл, содержащий данные исходного файла, в формате BASE 64;
5. Раскодировать из b64: создает файл, содержащий исходные данные файла, раскодированного из формата BASE 64;
6. Добавить присоединенную подпись: создает файл, содержащий присоединенную подпись исходного файла. При обработке файла, содержащего присоединенные подписи, новая подпись будет добавлена к существующим;
7. Проверить присоединенную подпись: выполняет проверку присоединенных подписей, содержащихся в файле. В случае успеха исходный файл перемещается в выходной каталог;
8. Проверить и Удалить присоединённую подпись: выполняет проверку присоединенных подписей, содержащихся в файле, и в случае успеха удаляет из файла все подписи и создает исходный файл в выходном каталоге;
9. Переместить: перемещает файлы из входного каталога в выходной. Если задать дополнительный выходной каталог с помощью кнопки «Доп. выходная папка», исходный файл также будет скопирован в этот каталог. Для копирова-

ния файла в несколько каталогов следует создать ряд правил, выполняющих последовательное перемещение и копирование файла в заданные каталоги. Существует возможность добавлять и удалять расширения перемещаемых файлов, а также создавать подкаталоги отчетности;

10. Удалить: удаляет файлы из входного каталога;

11. Зашифровать большой файл: потоковая версия операции «Зашифровать», работающая медленнее последней, но способная обрабатывать файлы любого размера;

12. Расшифровать большой файл: потоковая версия операции «Расшифровать», работающая медленнее последней, но способная обрабатывать файлы любого размера;

13. Создать отсоединённую подпись: создает отсоединённую подпись исходного файла. Данная операция предназначена только для создания первой отсоединённой подписи файла. Для добавления отсоединённой подписи к уже существующим, необходимо воспользоваться операцией «Добавить отсоединённую подпись». В случае успеха исходный файл перемещается в выходной каталог;

14. Добавить отсоединённую подпись: добавляет отсоединённую подпись к существующим подписям исходного файла. Обрабатывает пары файлов в формате «х.у» + «х.у.з», где «х» — имя исходного файла, «у» — расширение исходного файла, «з» — расширение файлов, содержащих отсоединённые подписи. Программа не будет обрабатывать файлы, для которых не будет подобрана пара. Непарные файлы будут оставаться во входном каталоге до появления в нем файла подходящего формата. Данная операция предназначена только для добавления отсоединённых подписей к уже существующим. Для создания первой отсоединённой подписи файла, необходимо воспользоваться операцией «Создать отсоединённую подпись»;

15. Проверить отсоединённую подпись: выполняет проверку отсоединённых подписей файла. Обрабатывает пары файлов в формате, аналогичном операции «Добавить отсоединённую подпись» и так же не обрабатывает непарные файлы. В случае успеха исходные файлы перемещаются в выходной каталог;

16. Удалить подпись без проверки: удалить все присоединённые подписи файла без их проверки и создать исходный файл в выходном каталоге;

17. Переподписать: выполняет проверку существующих подписей файла (присоединённых или отсоединённых в зависимости от настроек правила) первой заданной ключевой системы, удаляет все подписи в случае успеха и добавляет подпись (присоединённую или отсоединённую) второй заданной ключевой системы (можно задать одну и ту же ключевую систему). В случае успеха операции переподписания в отсоединённый формат в выходном каталоге создается исходный файл. Данная операция позволяет выполнять переподписание файла на другой ключевой системе в оперативной памяти, исключая возможность компрометации исходного файла в процессе переподписания;

18. Добавить присоединённую подпись и зашифровать: создает файл, содержащий присоединённую подпись исходного файла, и зашифровывает его для заданного количества получателей. При обработке файла, содержащего присоединённые подписи, новая подпись будет добавлена к существующим;

19. Расшифровать, проверить и удалить присоединённую подпись: выполняет расшифрование, проверку присоединённых подписей, содержащихся в файле, и в случае успеха удаляет из файла все подписи и создает исходный файл в выходном каталоге;

20. Архивировать файл: выполняет сжатие файла в архив. Расширение результирующего файла настраивается в окне глобальных настроек программы;

21. Разархивировать файл: выполняет распаковку архива, содержащего один файл. Если в окне глобальных настроек программы указано расширение сжатых файлов, операция будет вести поиск и удаление этого расширения у результирующих файлов;

22. Упаковать файлы: выполняет сжатие и упаковку файлов из входного каталога в один архив в выходном каталоге. Для данной функции можно задать максимальный общий размер исходного содержимого архива, формат имён создаваемых архивов, количество файлов в архиве, а также установить время ожидания необходимого количества файлов в каталоге;

23. Распаковать файлы: выполняет распаковку файлов из архива, находящего во входном каталоге, в выходной каталог с возможностью создания подкаталогов;

24. Исполнить: исполняет заданную командную строку с возможностью выбрать исполняемый файл и параметры выполнения.

3.4.2 Работа с масками

Для добавления маски необходимо нажать кнопку «Создать» и в появившемся окне ввести новую маску или выбрать из выпадающего списка уже существующих масок (Рисунок 15). Маски, созданные пользователем для других правил, будут добавляться в начало списка.

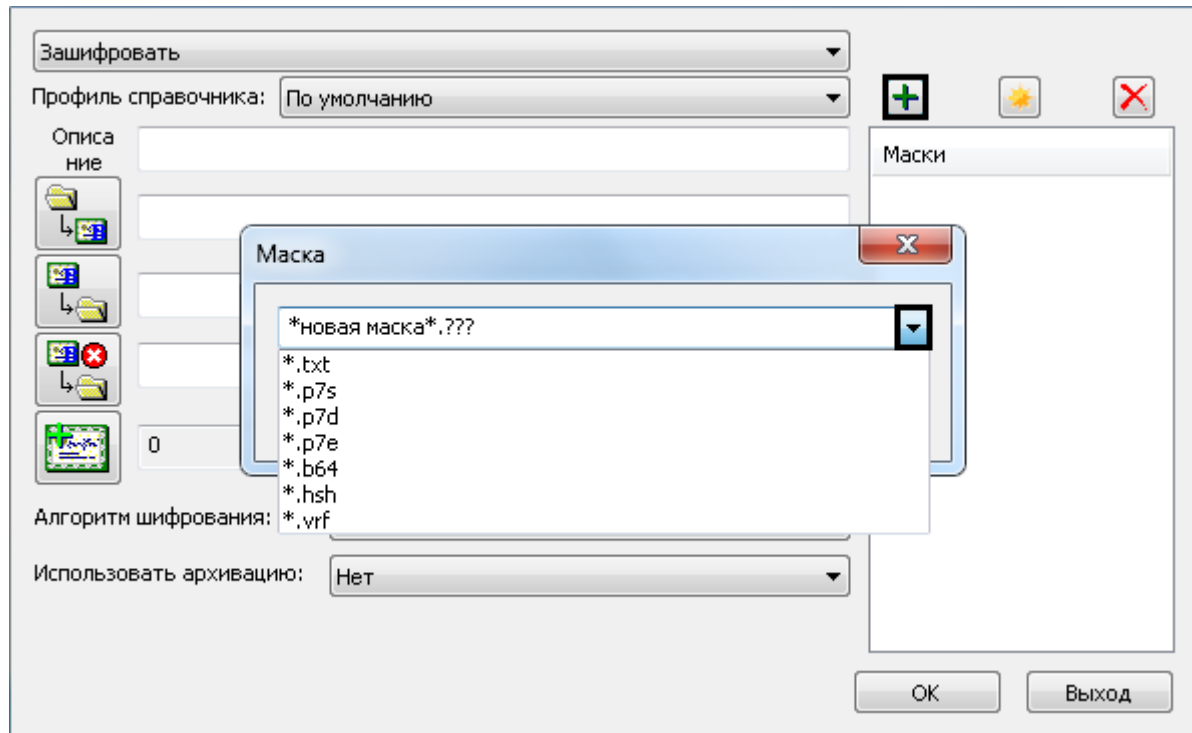


Рисунок 15 – Создание новой маски правила

Для редактирования существующей маски необходимо выбрать маску в списке и нажать кнопку «Изменить» (Рисунок 16).

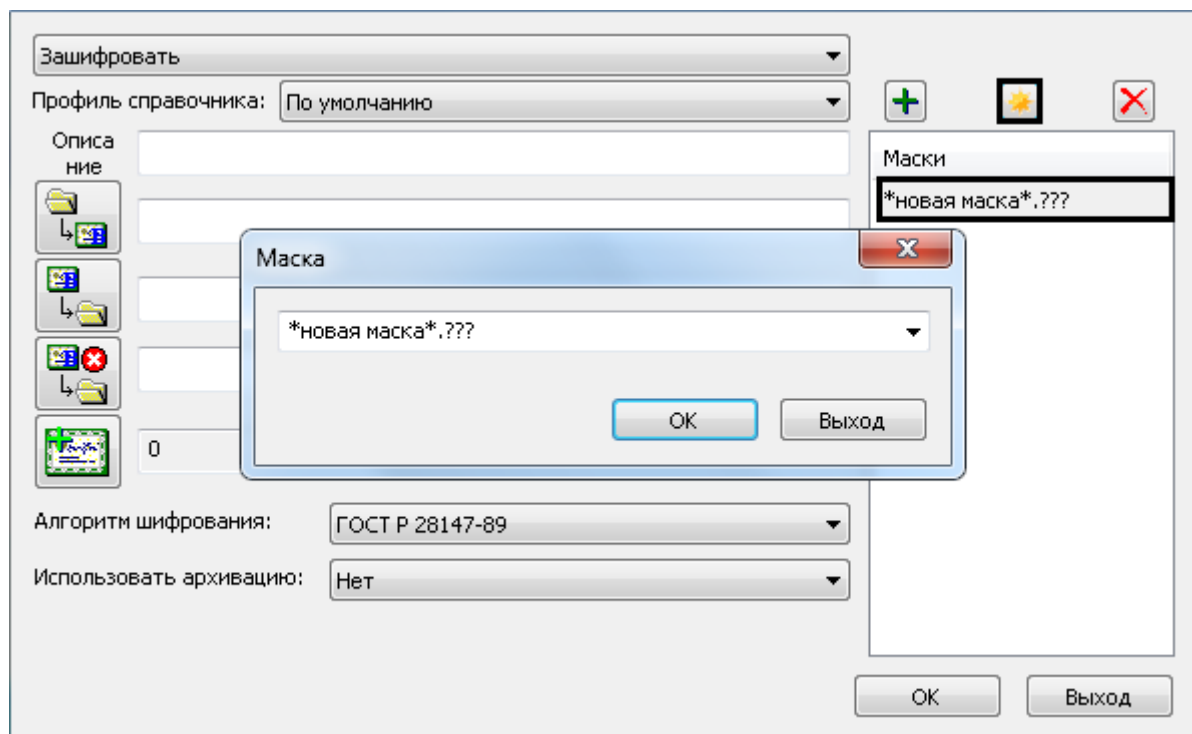


Рисунок 16 – Редактирование маски правила

Для удаления масок правила необходимо выбрать маски, подлежащие удалению, и нажать кнопку «Удалить» (Рисунок 17).

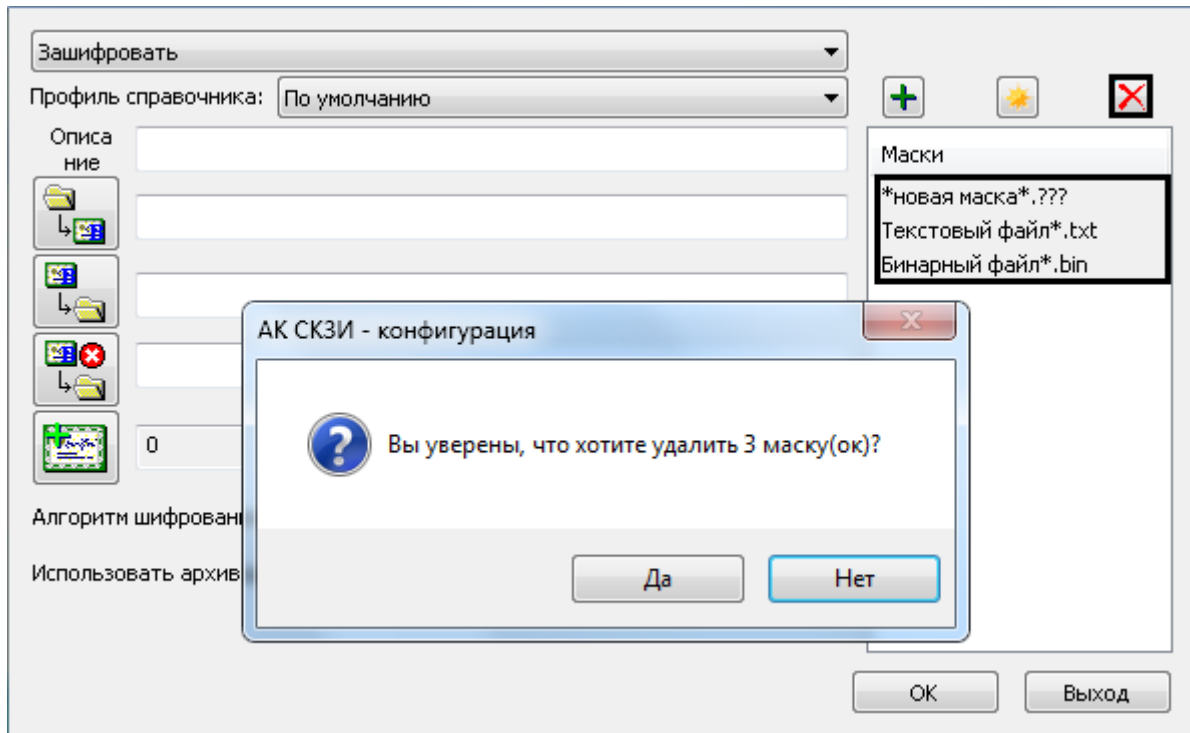


Рисунок 17 - Удаление масок правила

3.4.3 Работа с сертификатами получателей

Выбор сертификатов получателей, для которых будет производиться шифрование для в операциях «Зашифровать», «Зашифровать большой файл» и «Добавить присоединённую подпись и зашифровать», производится нажатием кнопки «Добавить получателей» (Рисунок 18). Сертификаты, не предназначенные для шифрования, или сертификаты с истекшим временем действия ключа будут исключаться из поиска.

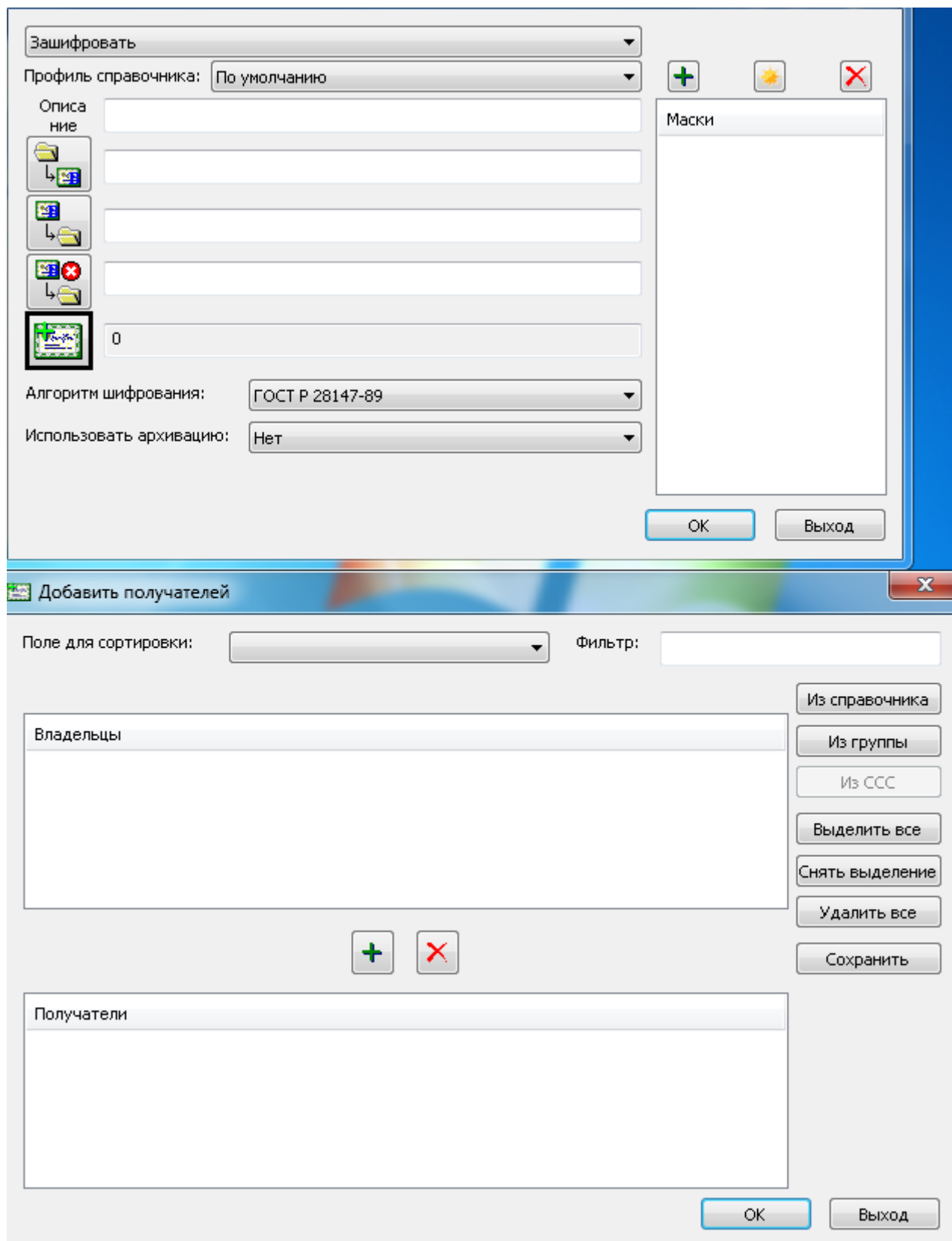


Рисунок 18 - Выбор сертификатов получателей

Окно добавления получателей позволяет:

- добавлять в список владельцев сертификаты из локального справочника нажатием кнопки «Из справочника»;

- добавлять в список владельцев сертификаты из сетевого справочника;
- сохранять сертификаты группами в файл;
- добавлять в список владельцев сертификаты группами из файла;
- выделять все сертификаты в списке владельцев нажатием кнопки «Выделить все»;
- снимать выделение со всех сертификатов в списке владельцев нажатием кнопки «Снять выделение»;
- удалять все выделенные сертификаты из списка владельцев нажатием кнопки «Удалить все»;
- искать нужные сертификаты в списке владельцев с помощью поля ввода «Фильтр»;
- сортировать сертификаты в списке владельцев с помощью выпадающего меню «Поле для сортировки»;
- добавлять выделенные сертификаты в список получателей из списка владельцев;
- удалять выделенные сертификаты из списка получателей.

Для работы с сетевым справочником в настройках профиля должно быть разрешено использование LDAP, отключенное по умолчанию. При инициализации криптопрофиля программа попытается подключиться к LDAP, в случае ошибки пользователю будет предложено продолжить работу без LDAP, в случае успеха в окне «Добавить получателей» станет доступна кнопка «Из LDAP», при нажатии которой отобразится окно фильтра. Для поиска владельцев сертификатов в сетевом справочнике пользователь должен выбрать поле справочника в выпадающем меню и шаблон, по которым будет проводиться поиск (Рисунок 19). Шаблон должен содержать хотя бы один символ кроме «*» и пробелов или быть равен «*» для поиска по всем владельцам по выбранному полю.

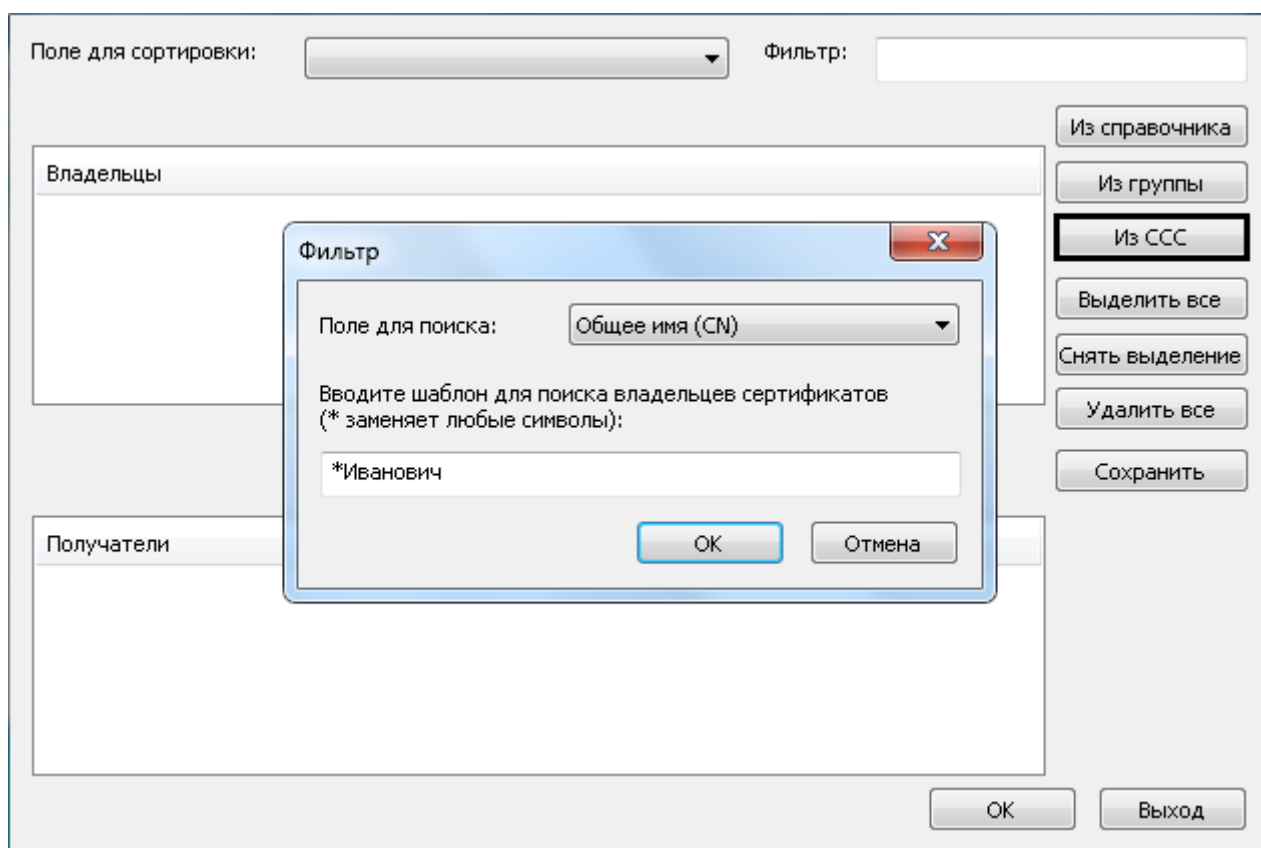


Рисунок 19 – Окно фильтра владельцев сертификатов в сетевом справочнике

Символ «*» заменяет любое количество символов, регистр букв значения не имеет. Вкладка меню «Поиск по всему имени» позволяет вести поиск по всему имени владельца. Для поиска по конкретным полям символ «*» добавляется в начале и конце шаблона, например, «GN=*Иван*,L=Москва» (порядок полей имеет значение). Шаблон «*» может использоваться как шаблон для поиска всех владельцев с таким полем сертификата. После нажатия кнопки «ОК» найденные в сетевом справочнике новые владельцы сертификатов будут добавлены в список владельцев.

Сохранение группы получателей в файл производится с помощью кнопки «Сохранить» (Рисунок 20).

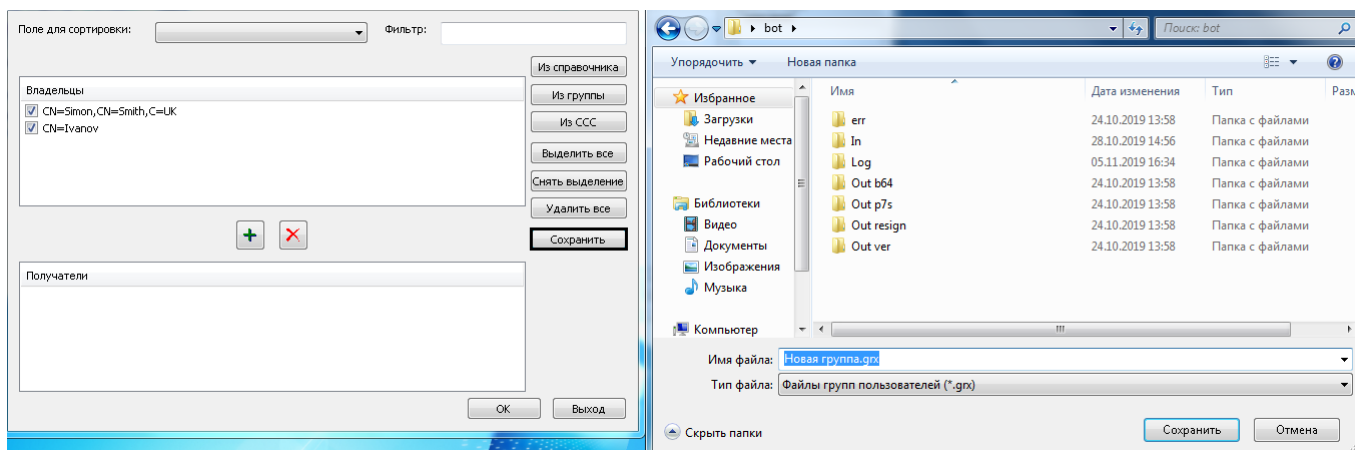


Рисунок 20 – Сохранение группы сертификатов получателей

Добавление в список владельцев сертификатов группами из файла производится нажатием кнопки «Из группы» и выбором нужного файла (Рисунок 21).

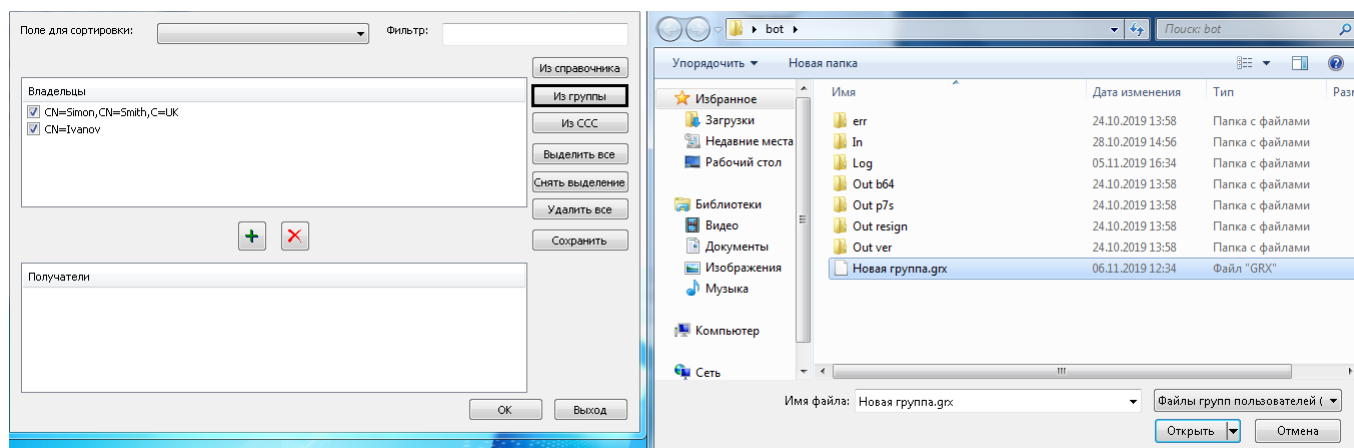


Рисунок 21 – Добавление группы сертификатов получателей

Добавление выделенных сертификатов в список получателей из списка владельцев производится с помощью кнопки «Добавить» (Рисунок 22).

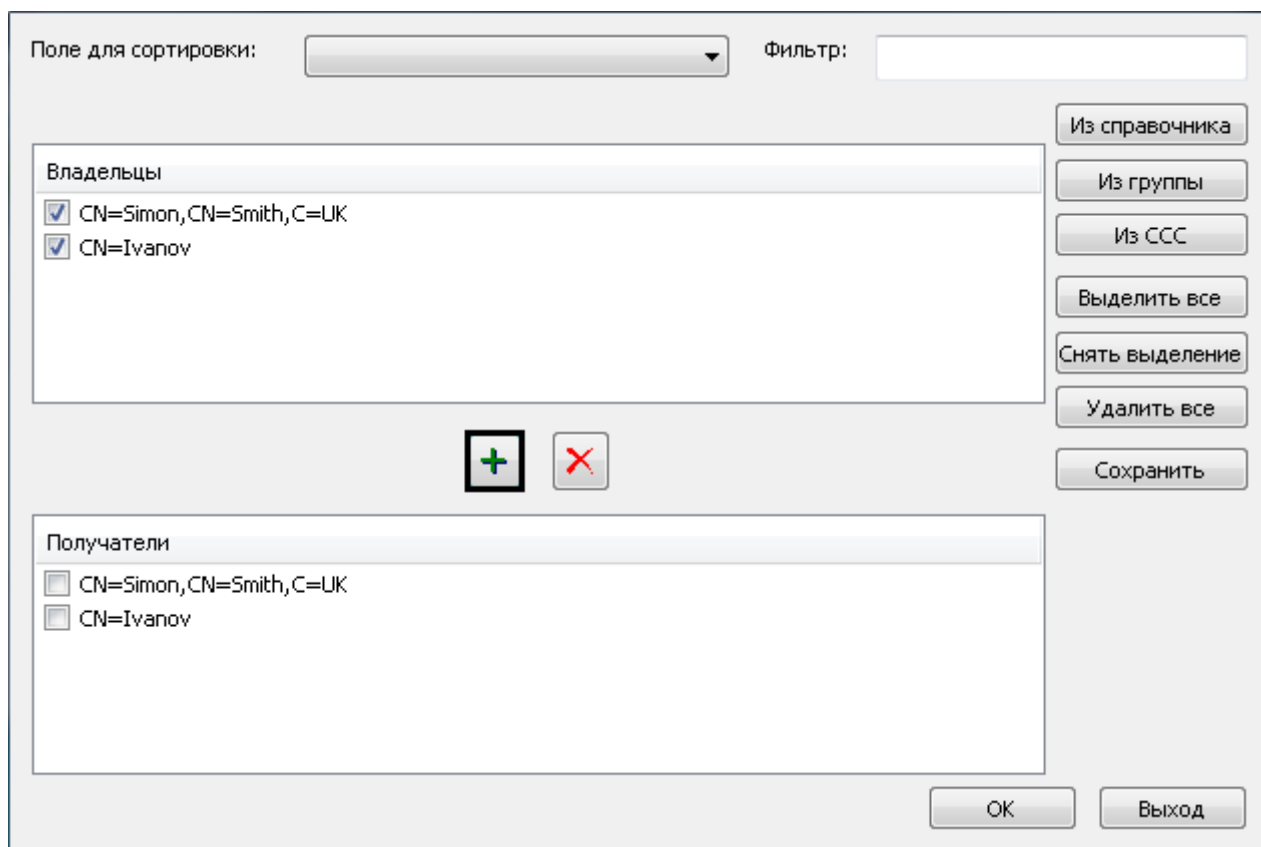


Рисунок 22 – Добавление сертификатов в список получателей

Удаление выделенных сертификатов из списка получателей производится с помощью кнопки «Удалить» (Рисунок 23).

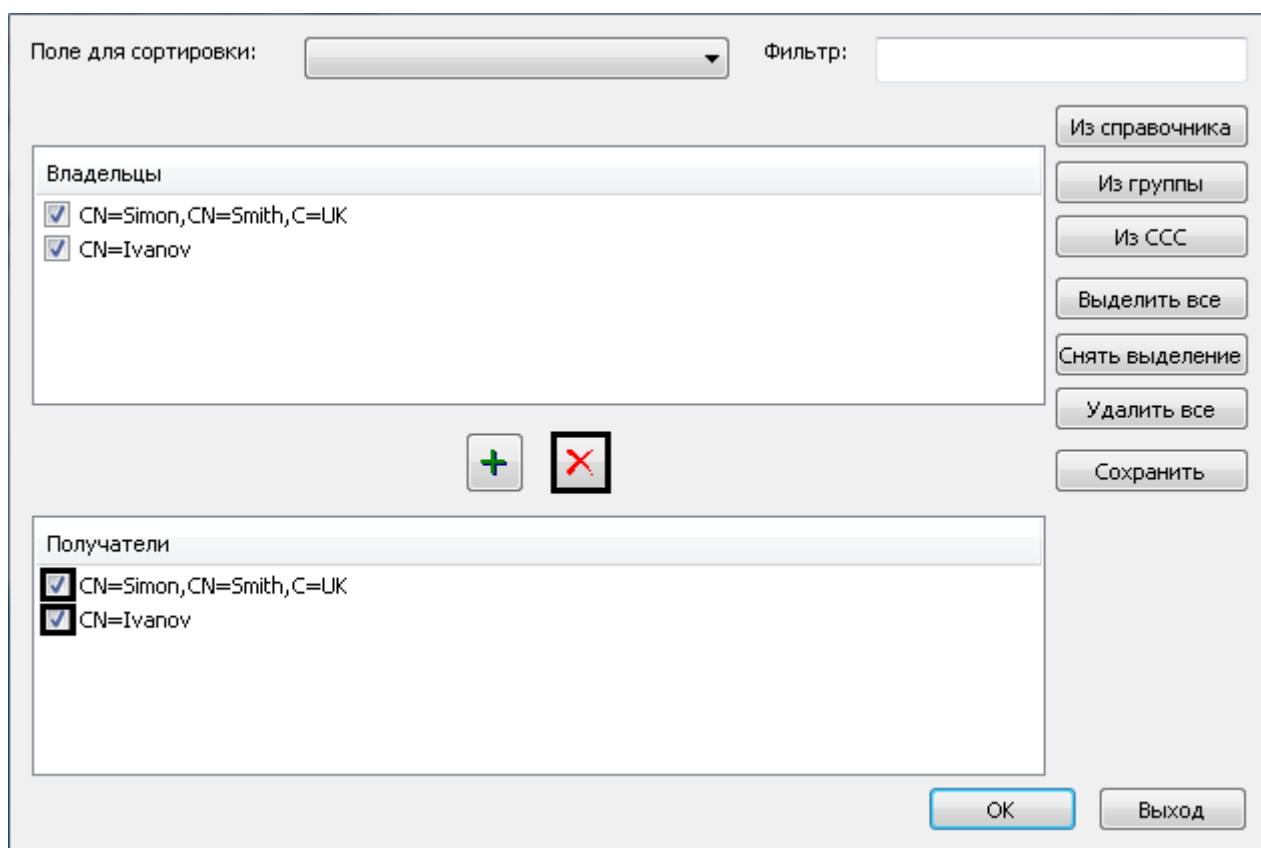


Рисунок 23 – Удаление сертификатов из списка получателей

Зашифрование будет проводиться для всех получателей из списка получателей.

3.4.4 Работа с параметрами операции «Переместить»

Для операции «Переместить» можно выбрать дополнительную выходную директорию для копирования файлов, расширения, которые будут удаляться или добавляться к перемещенным и скопированным файлам, а также задать формат подкаталогов отчетности (Рисунок 24).

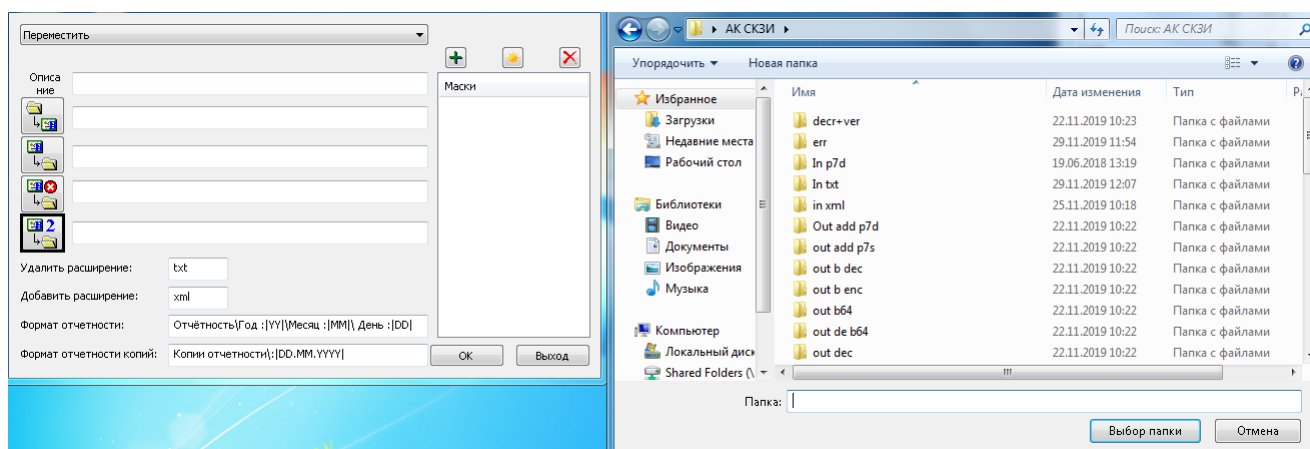


Рисунок 24 – Настройка правила «Переместить»

Дополнительная выходная директория для копирования файлов может быть

не задана, и в таком случае копирование файлов производиться не будет. Если это поле не будет пустым, программа будет провести его проверку. Выбор каталога для дополнительной директории производится с помощью кнопки «Доп. выходная папка».

Удаляемое расширение файлов задается с помощью поля ввода «Удалить расширение». Если поле будет задано, программа будет вести поиск и удаление заданного расширения в именах перемещенных и скопированных файлов.

Расширение, добавляемое к перемещенным и скопированным файлам, задается с помощью поля ввода «Добавить расширение».

Формат отчетности позволяет распределять файлы по подкаталогам, создаваемым программой в выходном и дополнительном выходном каталогах в соответствии с текущей датой. Для этого в строке «Формат отчетности» необходимо описать структуру подкаталогов, разделенных символами «\» или «/». Для использования в именах подкаталогов цифр, соответствующих текущей дате, необходимо воспользоваться специальной символьной структурой «:|...|», например, «:|YYYY.MM.DD|». Каждый символ «Y» или «y» внутри структуры будет заменён цифрой текущего года, начиная с последнего, большие и малые символы «M» и «D» цифрами месяца и дня соответственно. Количество символов не ограничено. Например, если в структуре будет присутствовать только два символа «Y», то при создании подкаталога в 2019 году они будут заменены цифрами «19». Если в структуре будет присутствовать больше символов чем цифр в текущей дате, например, «DDD», то 15 числа текущего месяца два первых с конца символа «D» структуры будут заменены цифрами «5» и «1» соответственно, а третий символ будет заменён нулем. Таким образом, структура «Отчетность\Год :|YY|\Месяц :|MM|\День :|DD|» 15 декабря 2019 года будет интерпретирована программой как «Отчетность\Год 19\Месяц 12\День 15».

3.4.5 Настройка архивации правил

Для операций «Зашифровать», «Расшифровать», «Зашифровать большой файл», «Расшифровать большой файл», «Добавить присоединённую подпись и зашифровать» и «Расшифровать, проверить и удалить присоединённую подпись» можно включить архивацию в формате ZIP или GZIP с помощью выпадающего меню «Использовать архивацию» (Рисунок 25).

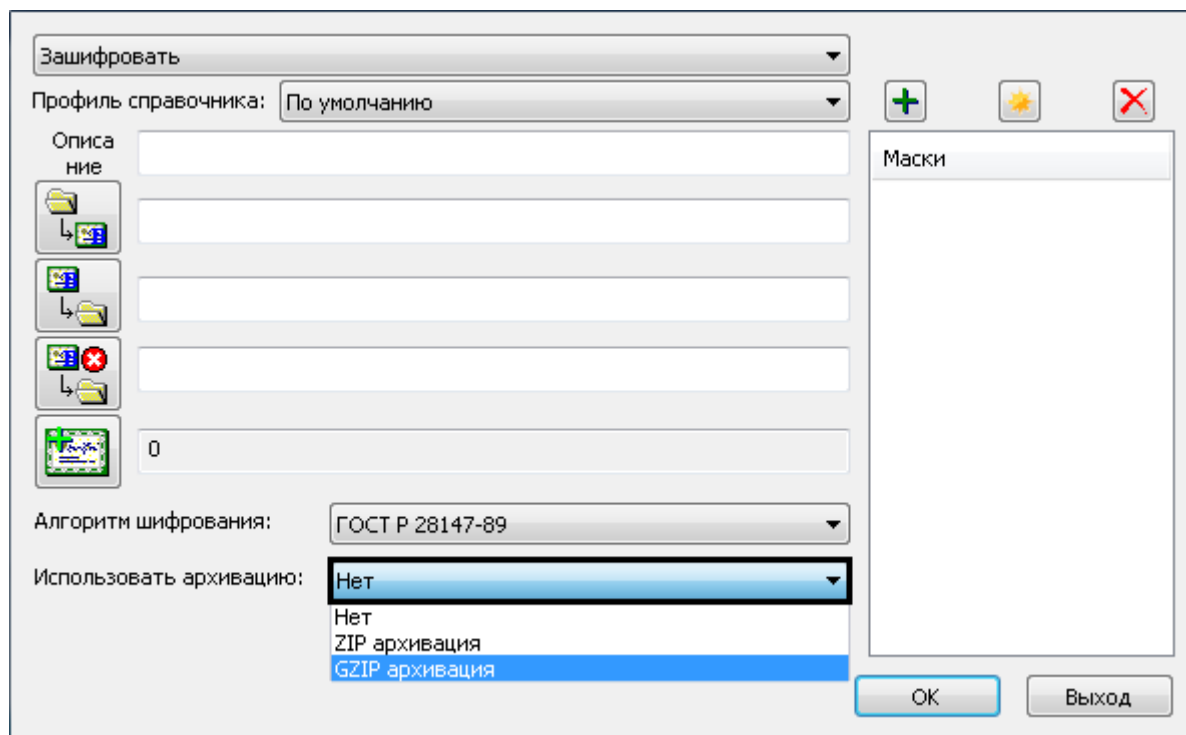


Рисунок 25 – Выбор формата архивации

3.4.6 Настройка типа операции подписания

Тип создаваемой подписи для операций «Добавить присоединённую подпись» и «Добавить присоединённую подпись и зашифровать» выбирается с помощью выпадающего меню «Тип операции» (Рисунок 26).

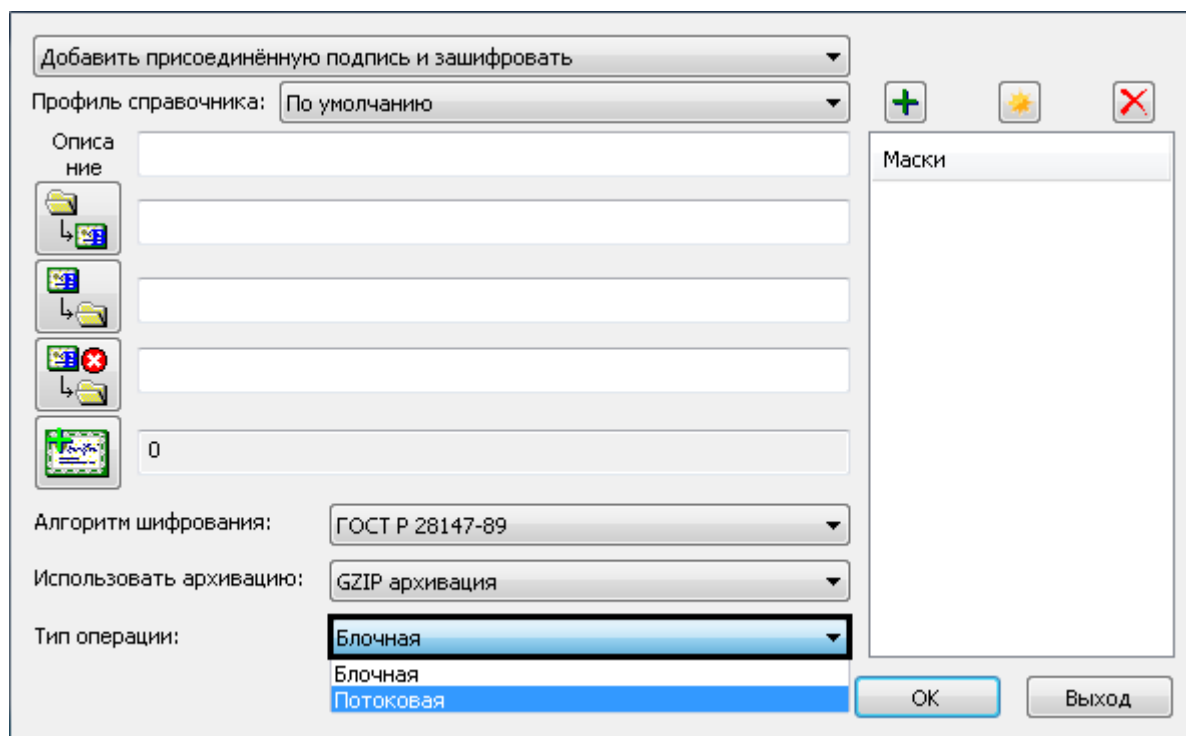


Рисунок 26 – Выбор типа создаваемой подписи

3.4.7 Работа с параметрами операции «Переподписать»

Для операции «Переподписать» существуют дополнительные параметры (Рисунок 27).

Переподписать

Профиль справочника: По умолчанию

Описание

Маски

Формат входной подписи: Присоединённая ЭП

Формат выходной подписи: Присоединённая ЭП

Новый профиль подписи: По умолчанию

OK Выход

Рисунок 27 – Дополнительные параметры функции «Переподписать»

Необходимо выбрать:

- формат входной подписи;
- формат выходной подписи;
- профиль справочника, используемого для добавления выходной подписи.

3.4.8 Работа с параметрами операции «Упаковать файлы»

Для операции «Упаковать файлы» можно выбрать дополнительные параметры (Рисунок 28).

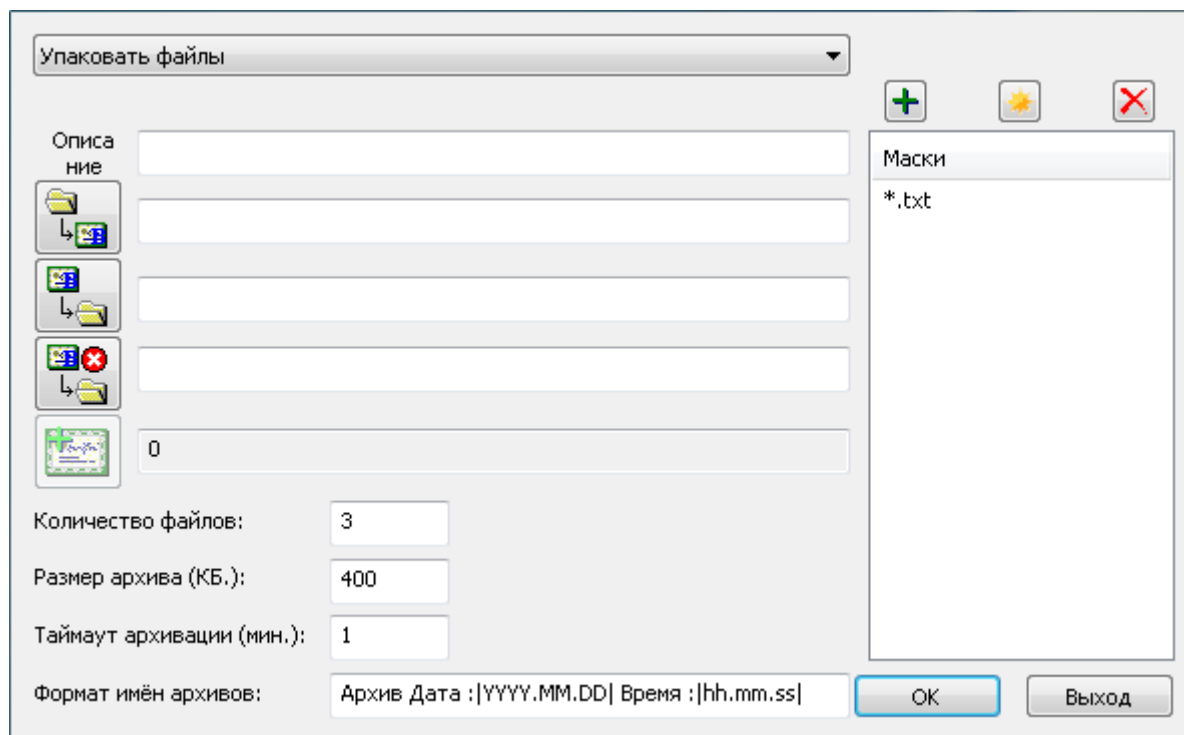


Рисунок 28 – Дополнительные параметры функции «Упаковать файлы»

Поле «Количество файлов» позволяет задать размер архива. Если количество файлов будет установлено выше нуля, программа будет ожидать появления во входном каталоге необходимого количества файлов. Поле ввода «Таймаут архивации» позволяет задать максимальное время этого ожидания, и, если оно истечет, программа упакует количество файлов, доступное на данный момент. Поле «Размер архивов» позволяет задать максимальный общий размер исходных данных в килобайтах, которые будут упакованы в архив. Файлы, чей размер превышает максимальный размер архива, будут пропускаться. Если ни один из этих параметров не будет задан, программа будет упаковывать все подходящие по маске файлы во входном каталоге. Поле «Формат имён архивов» позволяет создавать архивы с именами, содержащими текущую дату. Символьная структура «:| ... |» в этом поле работает так же, как в функции «Переместить», за исключением того, что регистр символов имеет значение, так как это поле также позволяет использовать символы «h», «m» и «s» как часы, минуты и секунды соответственно.

3.4.9 Работа с параметрами операции «Исполнить»

Для операции «Исполнить» необходимо выбрать исполняемый файл и указать параметры при необходимости (Рисунок 29).

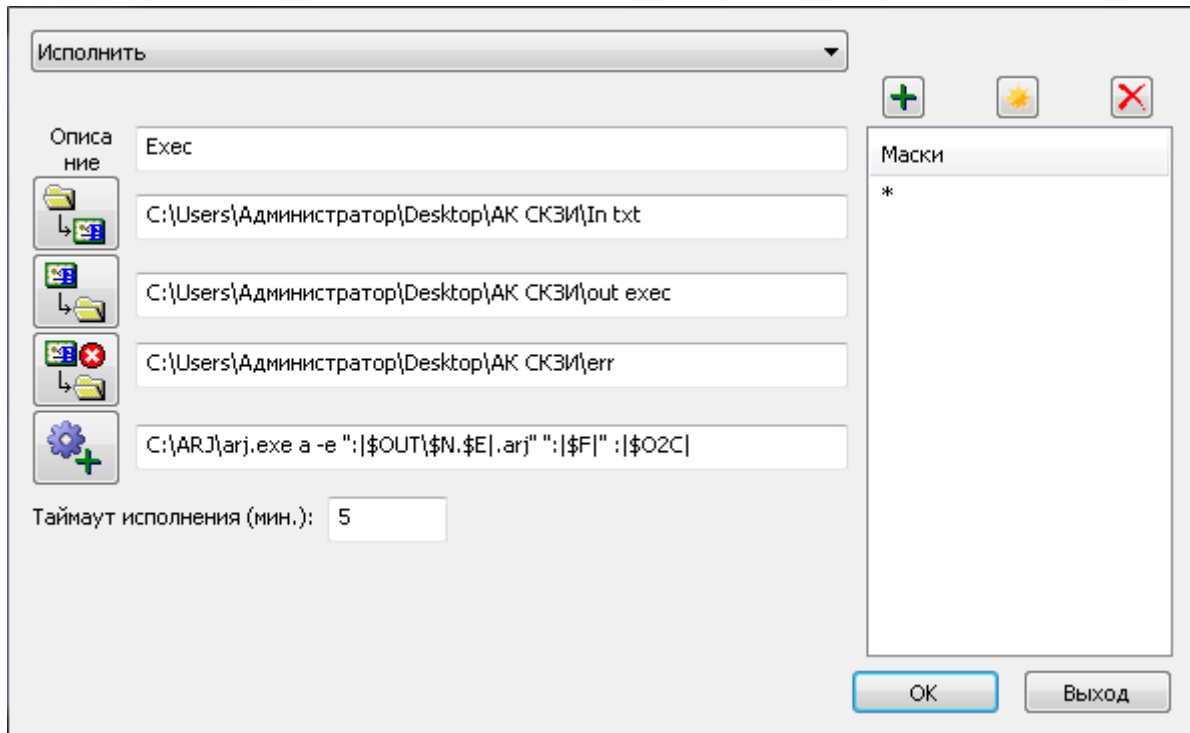


Рисунок 29 – Дополнительные параметры функции «Упаковать файлы»

В качестве параметров для исполняемого файла можно указать специальные ключи с помощью символьной структуры «:| ... |». При наличии пробелов в путях файлов эти пути необходимо выделять символами " ". Ключи «\$IN» и «\$OUT» будут заменены на входной и выходной каталоги соответственно. Ключ «\$F» будет заменен на полные имена файлов во входном каталоге. Ключи «\$N» и «\$E» будут заменены на имена файлов во входном каталоге и расширения этих файлов соответственно. Если в строке исполняемого файла будет использован ключ «\$F», «\$N» или «\$E», исполняемый файл будет применён ко всем файлам во входном каталоге. В противном случае исполняемый файл будет применён один раз. Остальные ключи не влияют на количество исполнений файла. Строка исполнения передается файлу в формате UTF-8. Так как некоторые программы используют формат Unicode, для работы с ними необходимо добавить дополнительный ключ «\$O2C». Символьная структура позволяет использовать ключи времени так же, как в функции «Упаковать файлы». Ключи времени необходимо заключать в отдельные символьные структуры во избежание ошибок интерпретации командной строки.

Поле «Таймаут исполнения» позволяет установить время ожидания завершения процесса исполняемого файла в минутах. В случае если таймаут равен нулю, программа будет ожидать завершения процесса бесконечно.

3.4.10 Работа со списками подписантов

Для операций «Проверить присоединённую подпись», «Проверить и Удалить присоединённую подпись», «Проверить отсоединённую подпись», «Переподписать» и «Расшифровать, проверить и удалить присоединённую подпись» можно добавить списки подписантов нажатием кнопки «Добавить подписантов» (Рисунок 30).

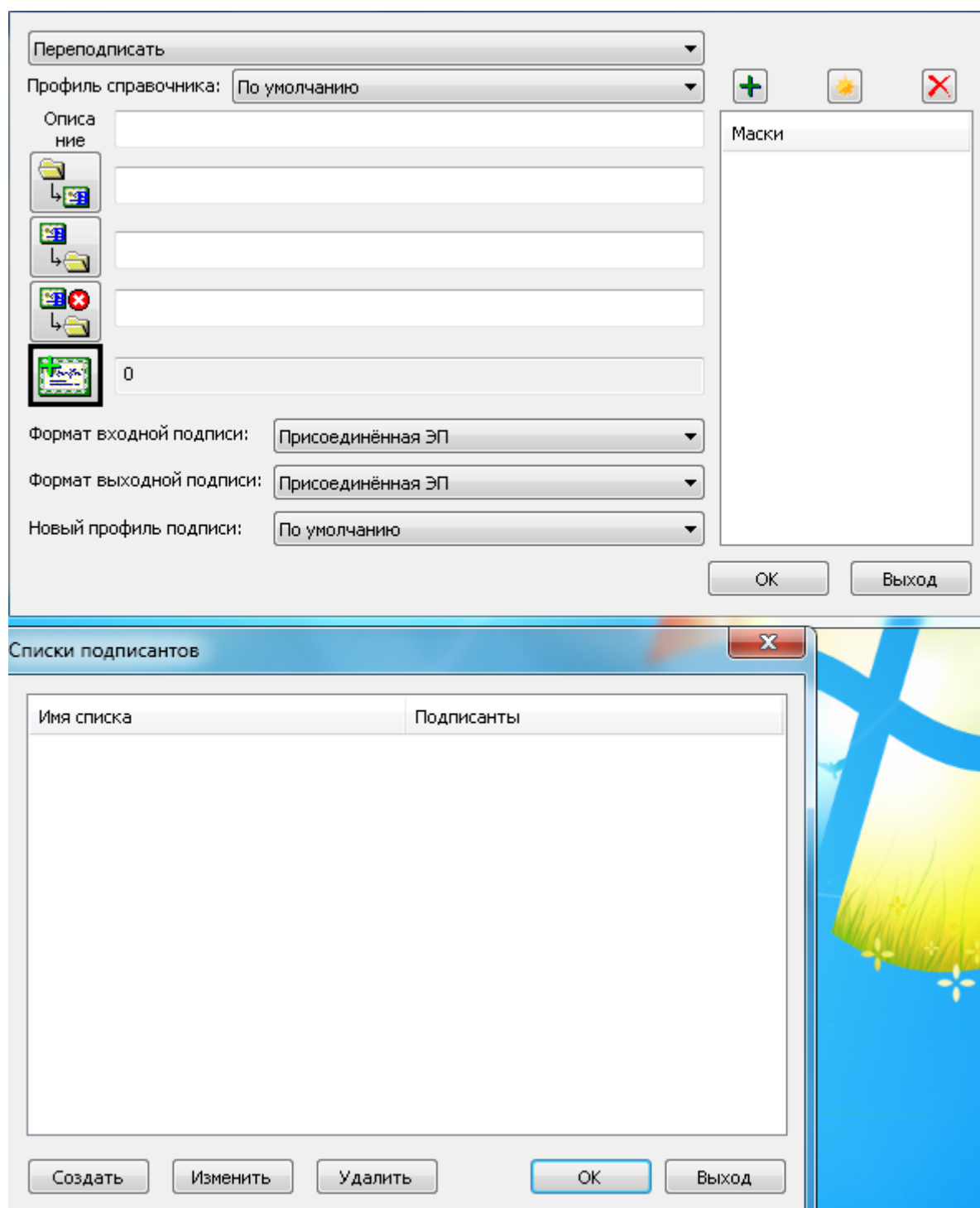


Рисунок 30 – Окно добавления списков подписантов

Списки подписантов позволяют задать необходимых подписантов, без подписи которых операция проверки подписи будет завершаться ошибкой. Программа будет искать в файле хотя бы одну подпись из каждого списка подписантов. Если количество списков подписантов будет превышать количество подписей в файле, операция завершится ошибкой. Каждый подписант может присутствовать только в одном списке подписантов одновременно.

Для создания списка подписантов необходимо нажать кнопку «Создать» (Рисунок 31). Отобразившееся окно добавления подписантов функционирует иден-

точно окну «Добавить получателей» с добавленным полем ввода для имени списка. Выбранные сертификаты будут добавлены в список и станут недоступны для выбора при создании и редактировании других списков подписантов.

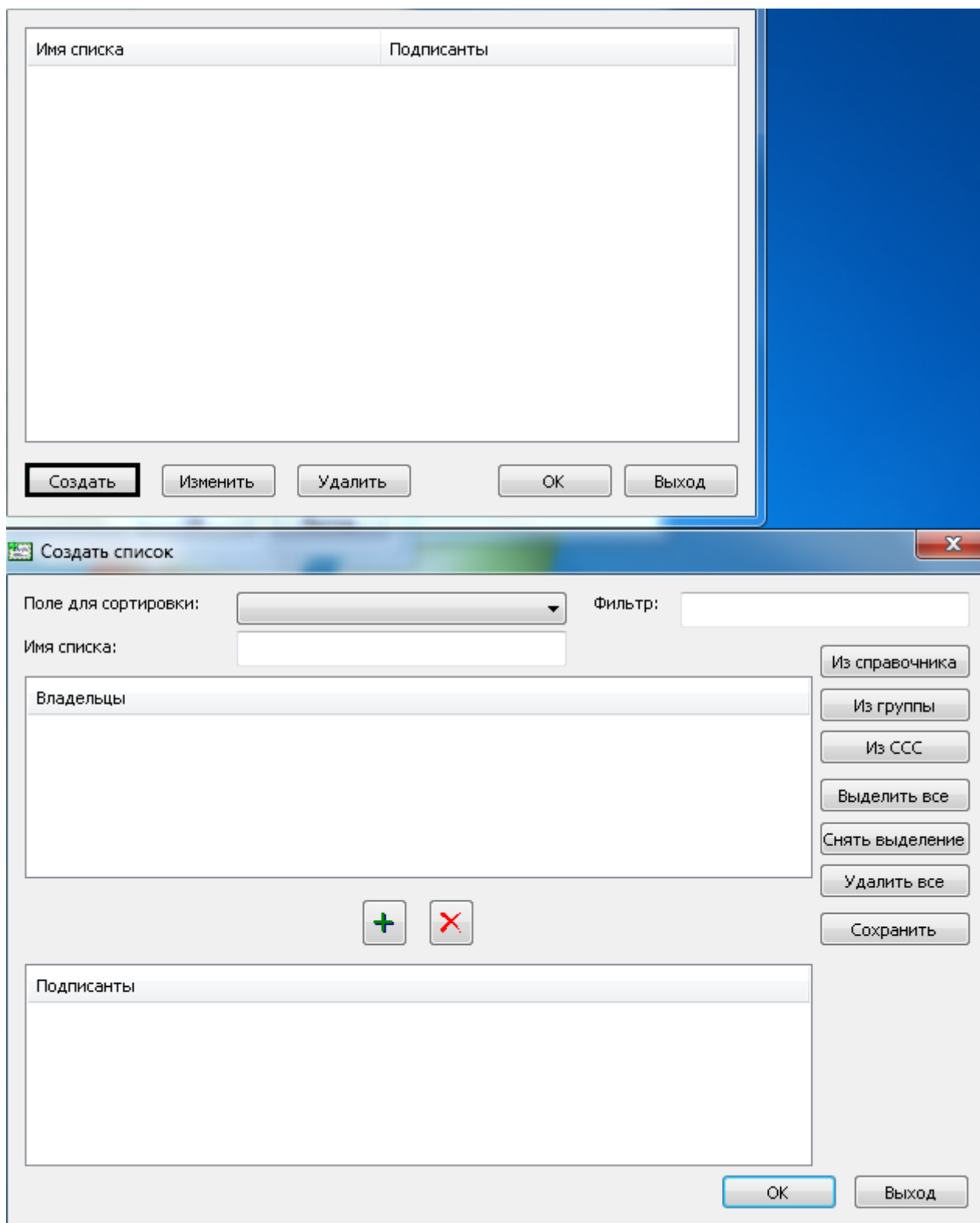


Рисунок 31 – Создание списка подписантов

Для редактирования списка подписантов необходимо выбрать список и на-

жать кнопку «Изменить» или дважды нажать на него левой кнопкой мыши (Рисунок 32).

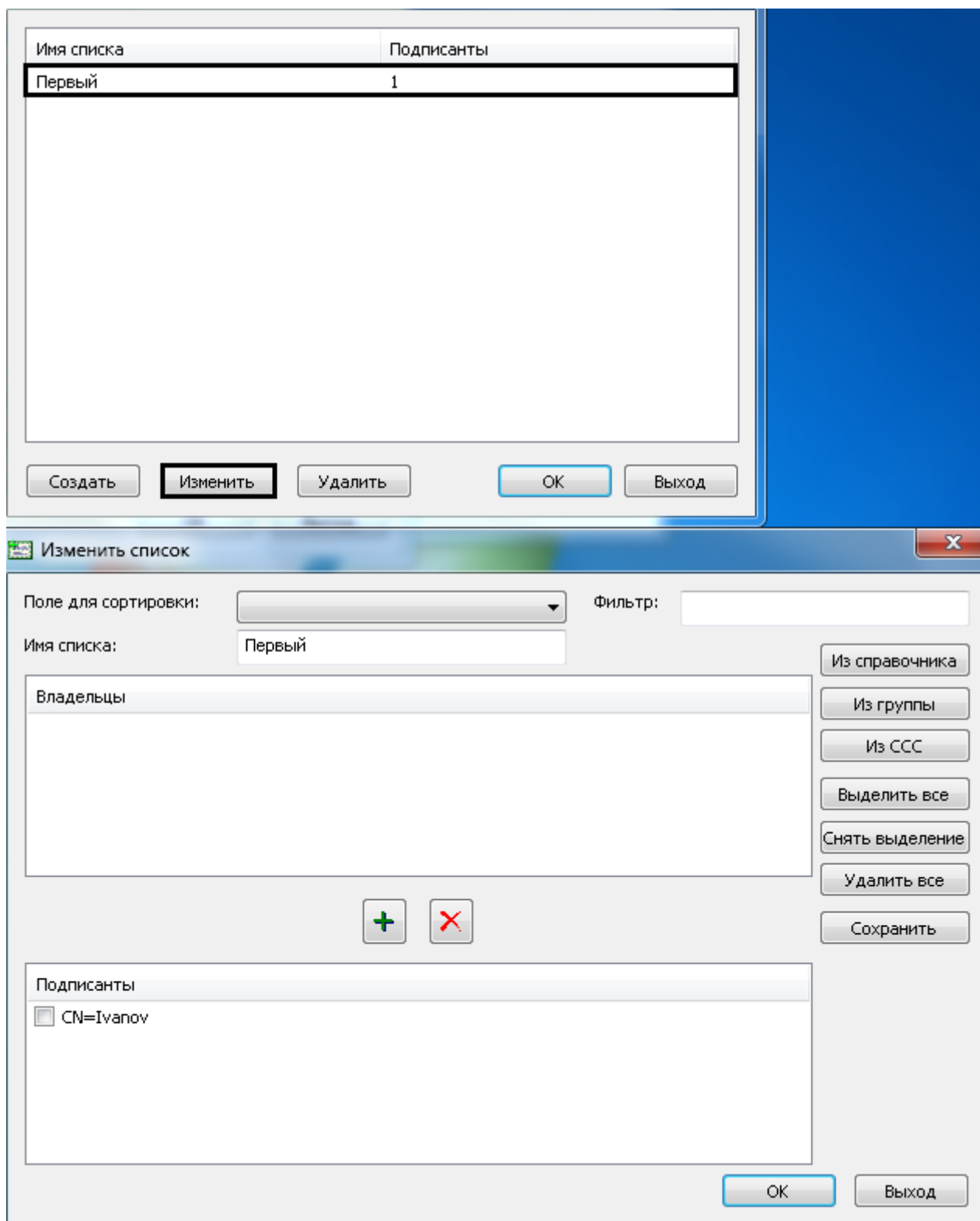


Рисунок 32 – Изменение списка подписантов

Для быстрого получения информации о списке подписантов необходимо нажать на него правой кнопкой мыши (Рисунок 33).

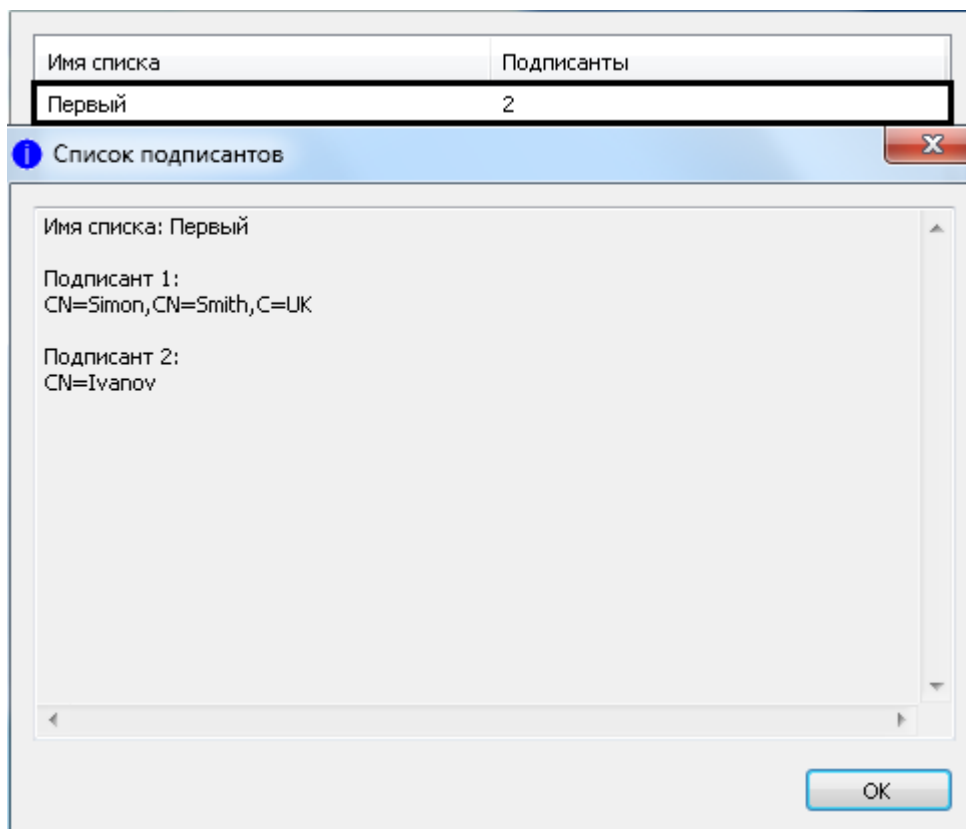


Рисунок 33 - Информация о списке

Для удаления списков подписантов необходимо выбрать списки, подлежащие удалению, и нажать кнопку «Удалить» (Рисунок 34).

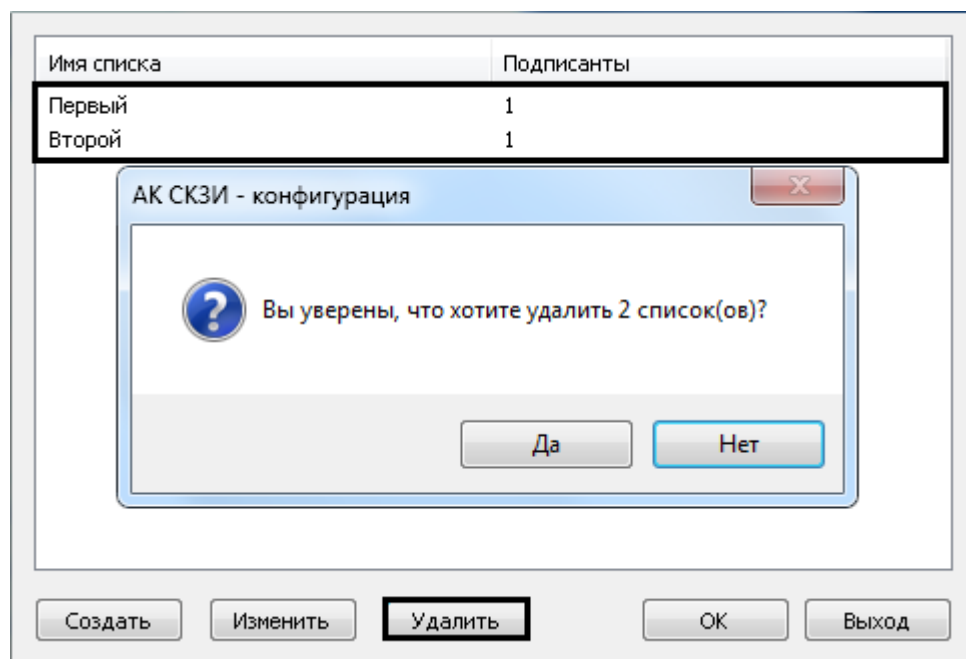


Рисунок 34 - Удаление списков подписантов

3.4.11 Описание правил

С помощью поля «Описание» (Рисунок 35) пользователь может добавить комментарий к правилу, по которому в дальнейшем можно будет вести поиск по правилам.

Рисунок 35 – Добавление описания к правилу

3.4.12 Копирование правил

Для копирования правил необходимо выбрать правило, которое требуется скопировать, и нажать кнопку «Копировать правило» (Рисунок 36), после чего копия правила будет добавлена следующей после выбранного правила.

	Описание	Правила	Входная п...	Выходная ...	Папка оши...	Маски	Профиль с...	Дополните...	
<input checked="" type="checkbox"/>	1	Присоедин...	Добавить ...	C:\Users\A...	C:\Users\A...	C:\Users\A...	*.txt	По умолча...	Блочная
<input checked="" type="checkbox"/>	2	Переподпи...	Переподпи...	C:\Users\A...	C:\Users\A...	C:\Users\A...	*.p7s	По умолча...	2; По умол...
<input checked="" type="checkbox"/>	3	Проверка	Проверить...	C:\Users\A...	C:\Users\A...	C:\Users\A...	*.p7s	По умолча...	
<input checked="" type="checkbox"/>	4	Закодиров...	Закодиров...	C:\Users\A...	C:\Users\A...	C:\Users\A...	*.p7s		

Рисунок 36 – Копирование правила

3.4.13 Редактирование правил

Для редактирования правил необходимо выбрать правило, требующее редактирования, и нажать кнопку «Редактировать правило..» или дважды щелкнуть по нему левой кнопкой мыши, после чего выбрать необходимые параметры (Рисунок 37).

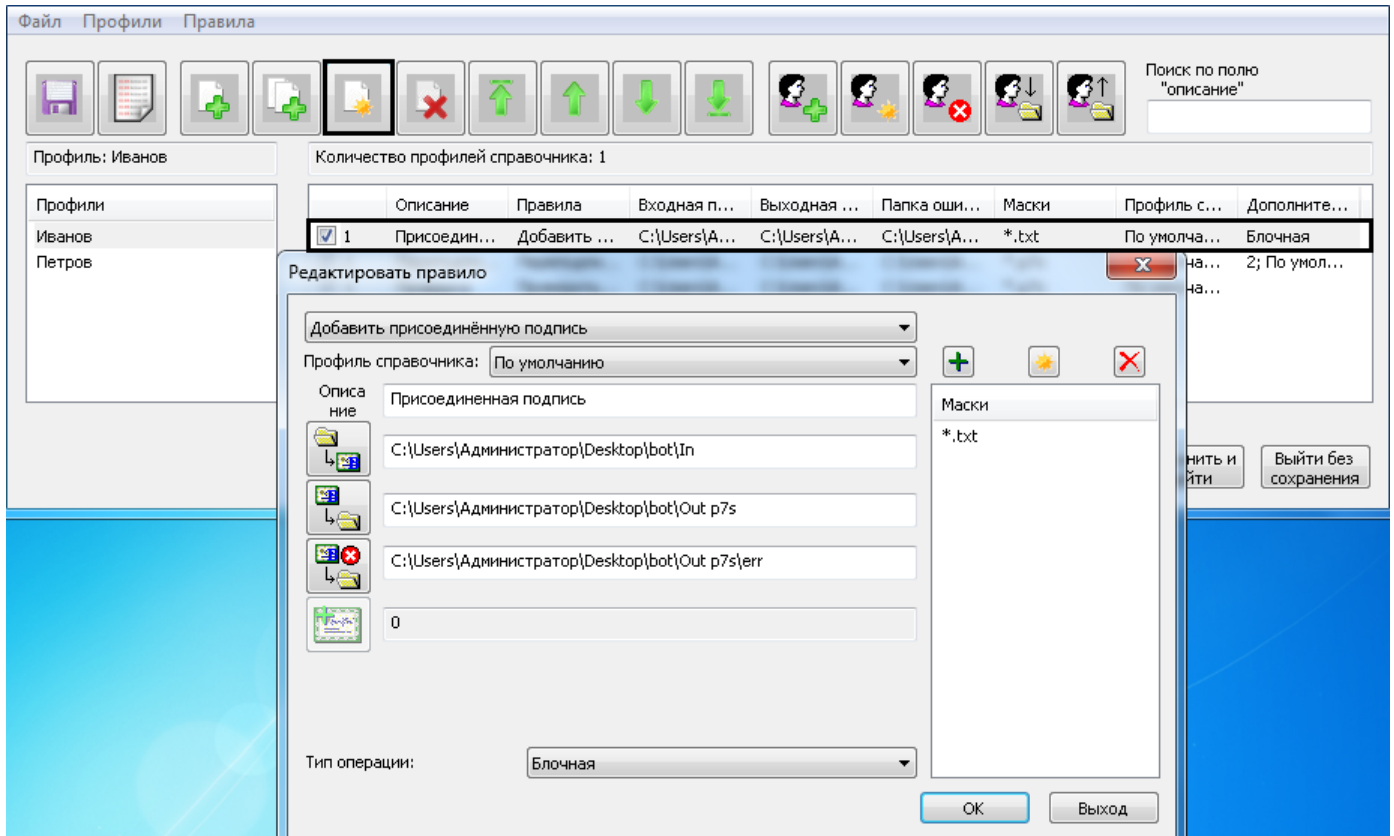


Рисунок 37 – Редактирование правила

3.4.14 Удаление правил

Для удаления правил необходимо выбрать удаляемые правила и нажать кнопку «Удалить правило» или клавишу «Delete» на клавиатуре (Рисунок 38).

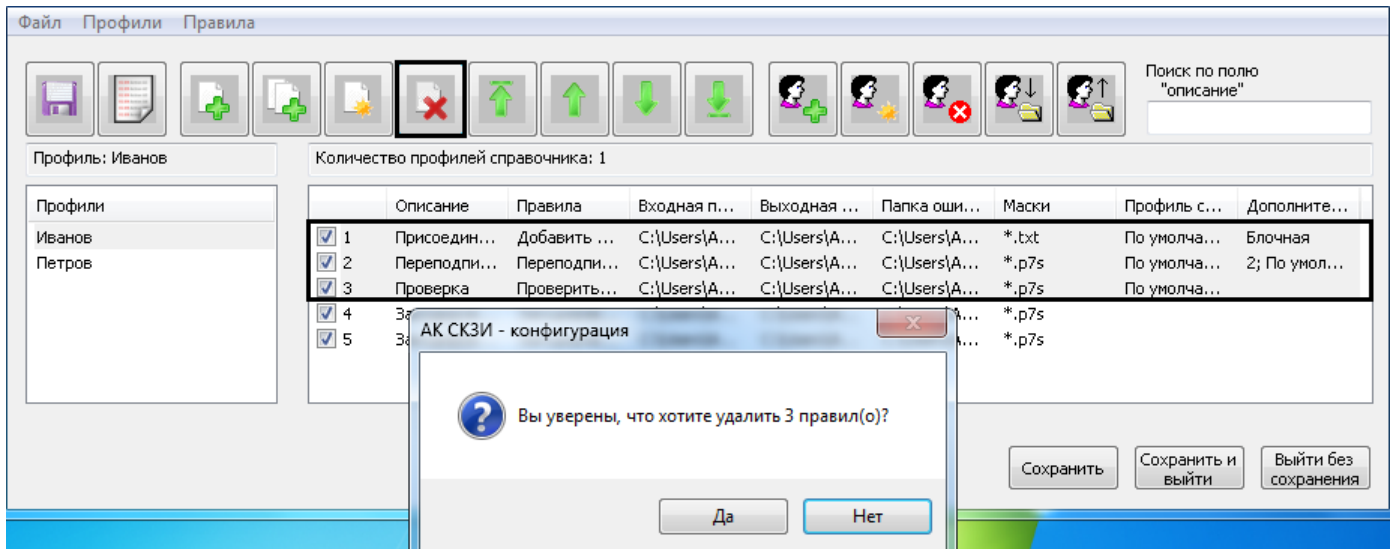


Рисунок 38 – Удаление правила

3.4.15 Изменение порядка исполнения правил

Правила применяются по порядку их последовательности в списке от первого до последнего. Чтобы изменить последовательность можно воспользоваться кнопками:

- «Сделать правило первым» передвинет правило в начало списка;
- «Сдвинуть правило вверх» передвинет правило на одну позицию вверх;
- «Сдвинуть правило вниз» передвинет правило на одну позицию вниз;
- «Сделать правило последним» передвинет правило в конец списка.

3.4.16 Временное отключение правил

Правило можно временно отключить, сняв «галочку» в его начале (Рисунок 39), и включить снова повторным нажатием.

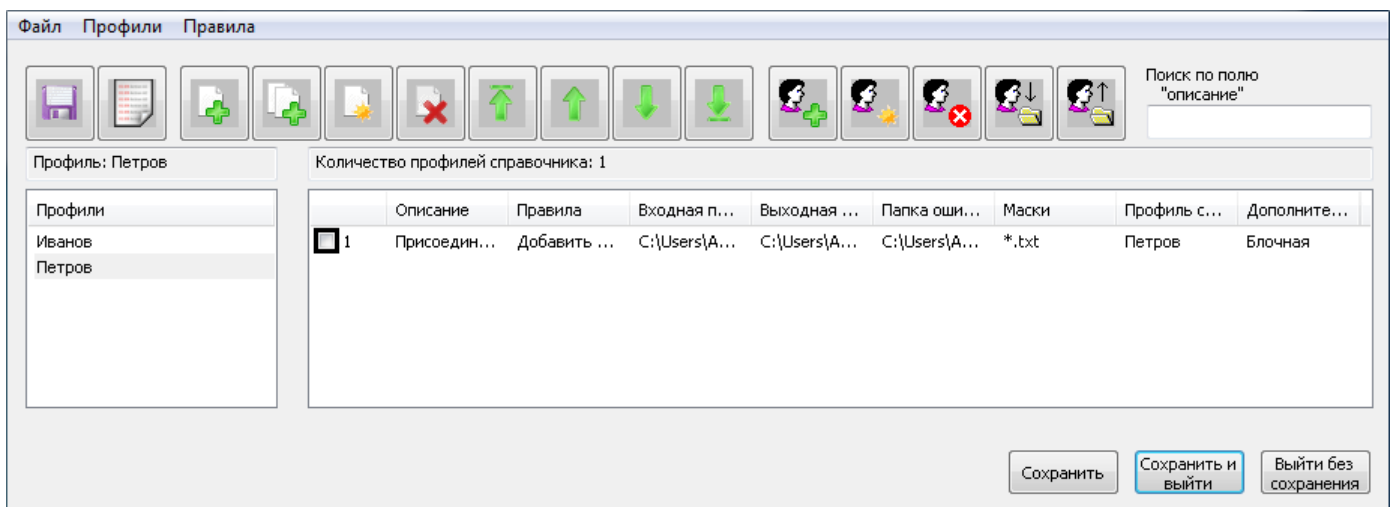


Рисунок 39 – Временное отключение правила

3.4.17 Отображение информации о пункте правила

Нажатие правой кнопкой мыши на пункт правила отобразит подробную информацию о нем (Рисунок 40).

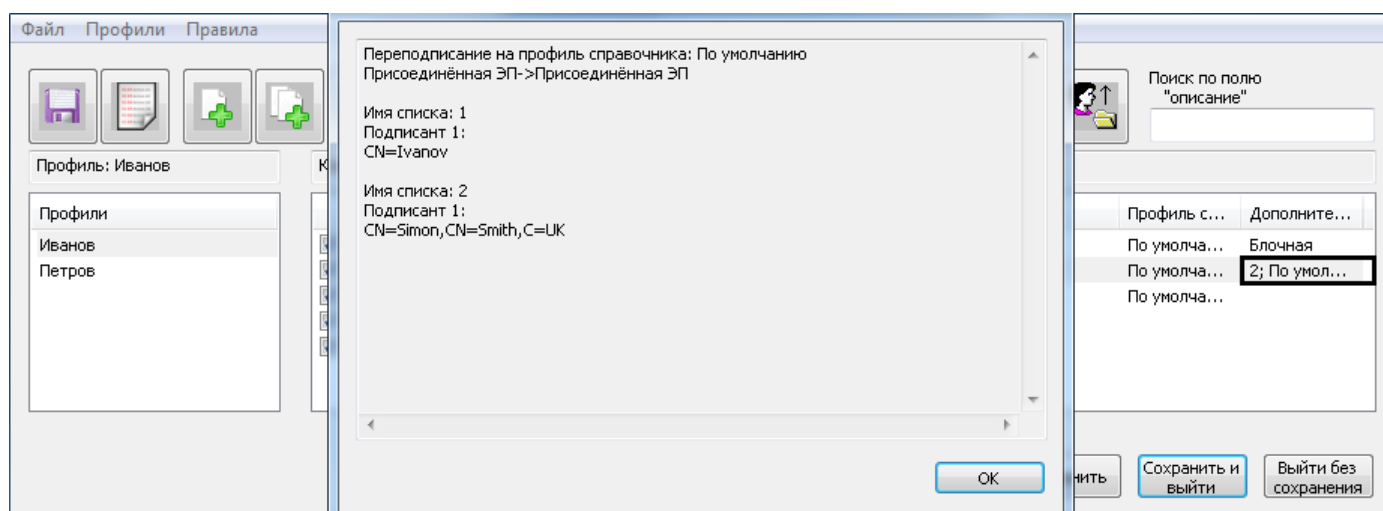


Рисунок 40 – Подробная информация о пункте правила

3.4.18 Экспорт правил профиля

Правила профиля можно сохранить в файл нажатием кнопки «Экспортировать профиль» (Рисунок 41).

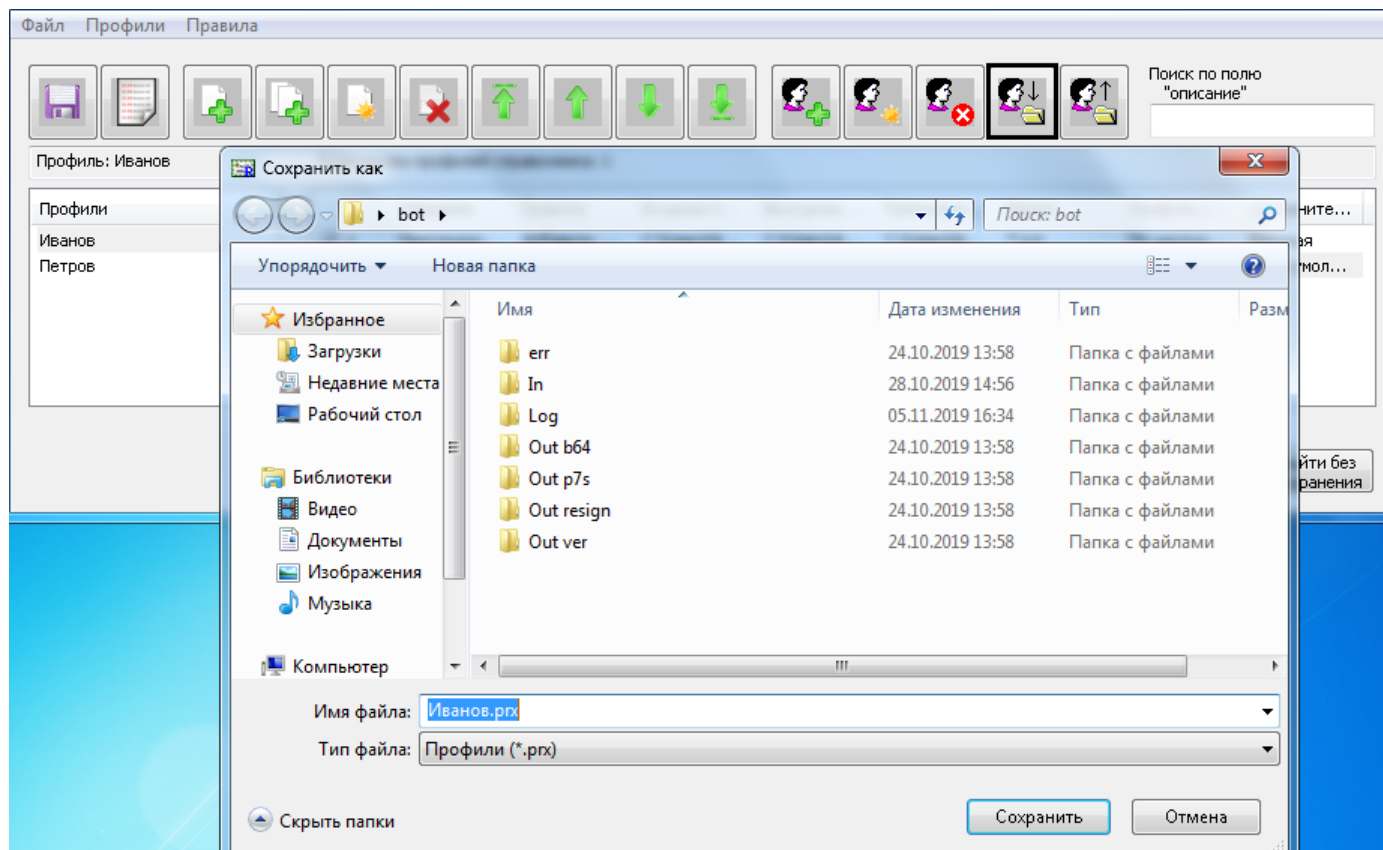


Рисунок 41 – Сохранение правил профиля в файл

3.4.19 Импорт правил профиля

Добавление правил профиля из файла происходит нажатием кнопки «Импортировать профиль» (Рисунок 42).

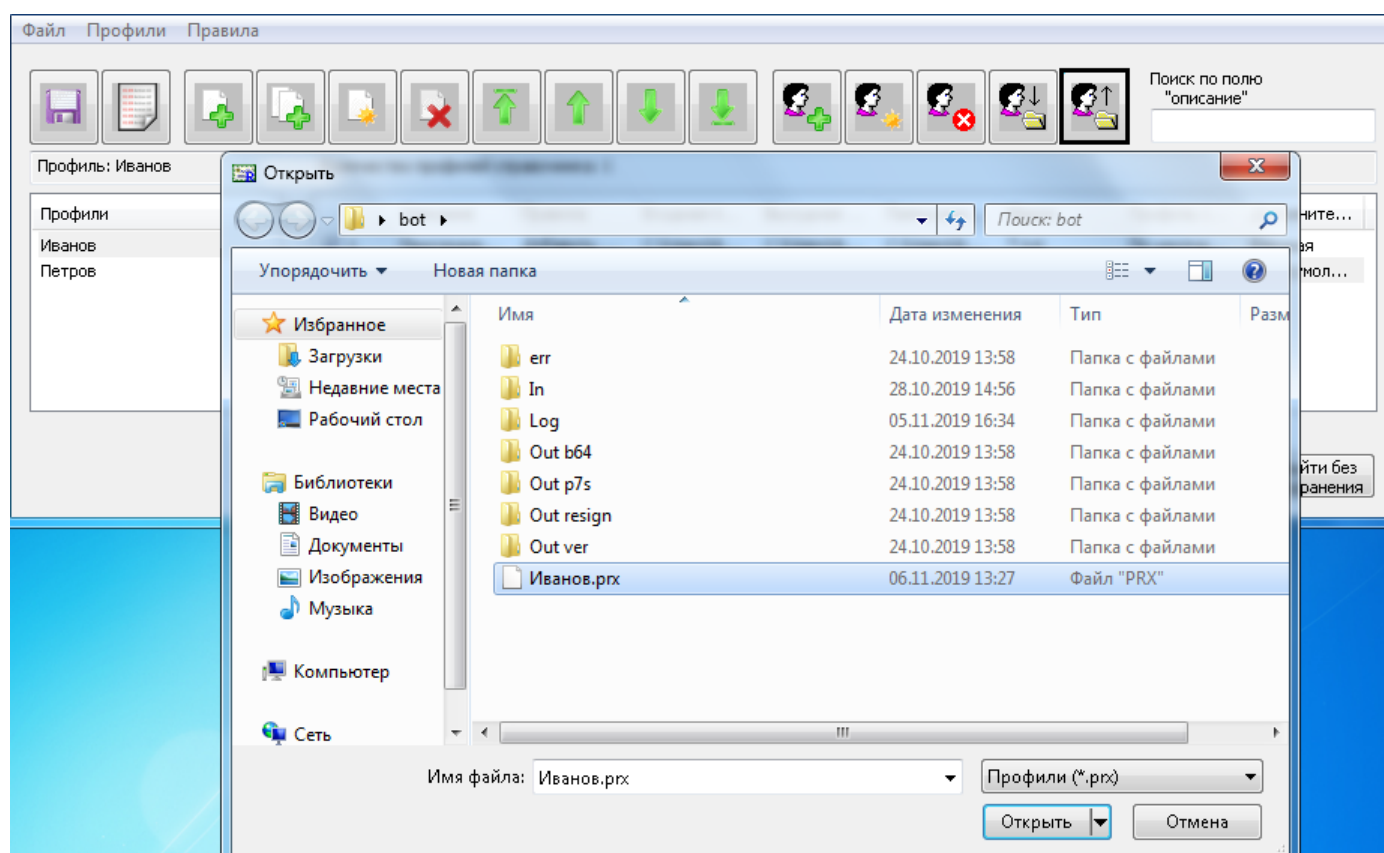


Рисунок 42 – Добавление правил профиля из файла

Внимание: после импортирования правил профиля из файла рекомендуется проверить сертификаты получателей и/или подписантов, если они присутствуют в импортированных правилах.

3.4.20 Поиск правил по описанию

С помощью поля «Поиск по полю Описание» можно вести поиск правил по описанию (Рисунок 43).

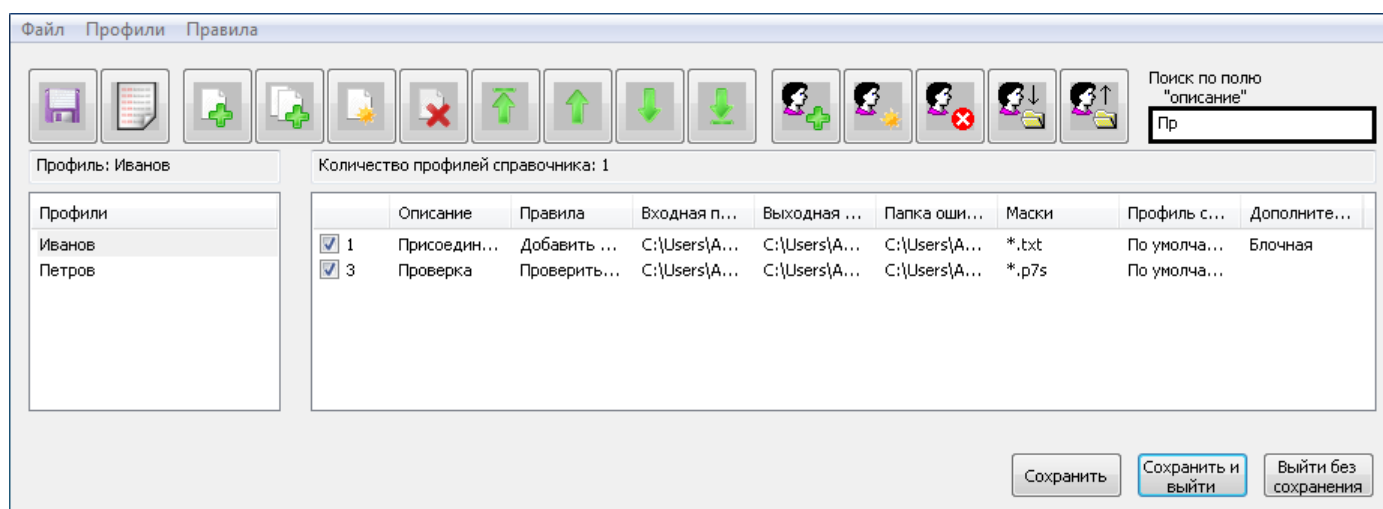


Рисунок 43 – Поиск правил по описанию

3.5 Сохранение внесенных изменений

Сохранение внесенных изменений выполняется нажатием кнопки «Сохранить» (Рисунок 44).

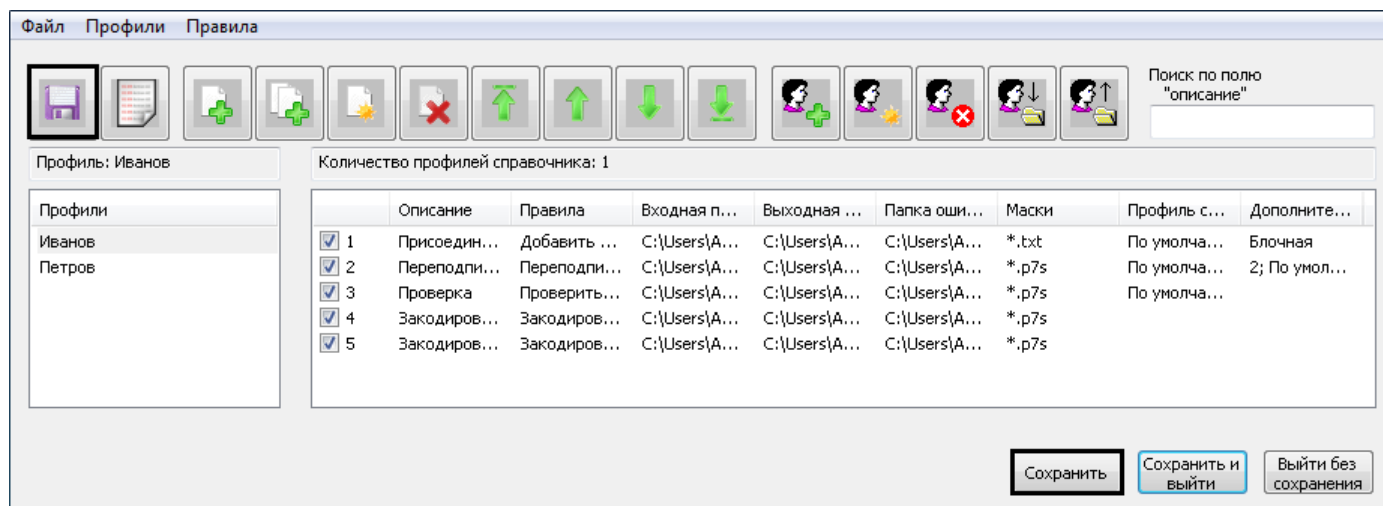


Рисунок 44 – Сохранение внесенных изменений

3.6 Выход из программы конфигурации

Выход из программы конфигурации можно осуществить:

- с сохранением изменений, нажав кнопку «Сохранить и выйти»;
- без сохранения изменений, нажав кнопку «Выйти без сохранения» или красную кнопку в правом верхнем углу программы.

При выходе без сохранения в случае наличия несохраненных данных будет отображен диалог с предложением сохранить изменения (Рисунок 45).

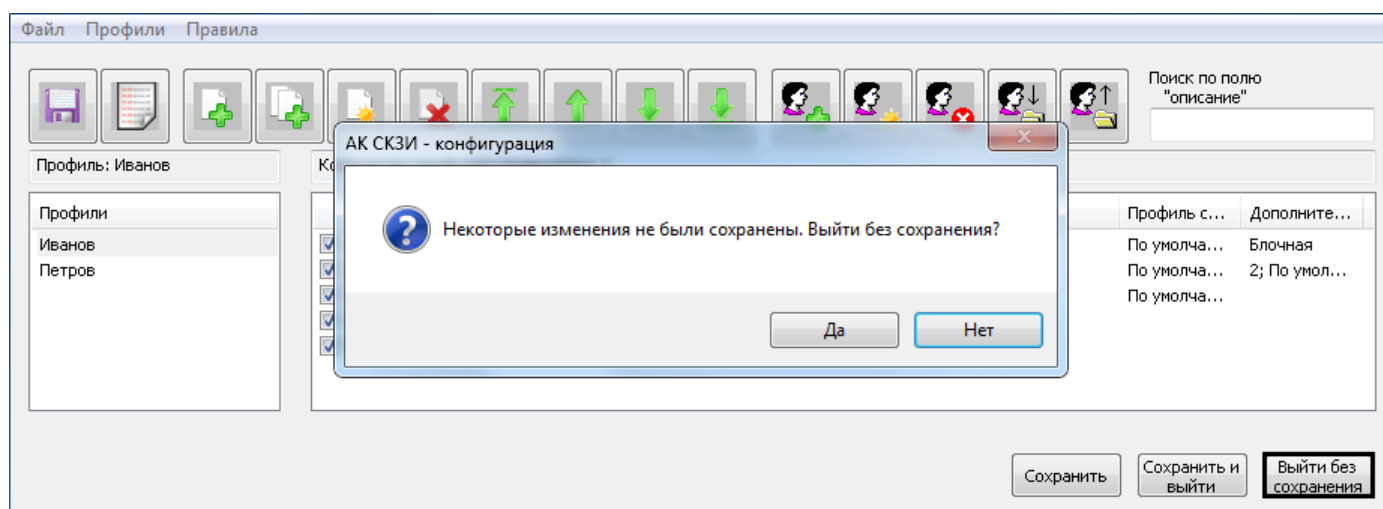


Рисунок 45 – Диалог с предложением сохранить изменения

3.7 Интерфейс обработчика ПК «АК СКЗИ»

Графический интерфейс обработчика ПК «АК СКЗИ» приведен на рисунке (Рисунок 46).

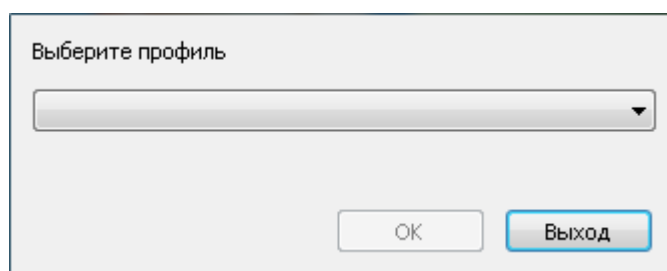


Рисунок 46 – Интерфейс обработчика ПК «АК СКЗИ»

3.8 Запуск обработчика ПК «АК СКЗИ»

Для запуска обработчика ПК «АК СКЗИ» необходимо выбрать один из профилей, созданных с помощью модуля конфигурации ПК «АК СКЗИ», и нажать кнопку «ОК», после чего программа перейдет в фоновый режим и создаст иконку в меню задач (Рисунок 47). Одновременно можно запускать несколько процессов обработки, однако, запустить больше одного обработчика с одним выбранным профилем нельзя.

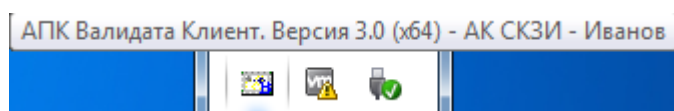


Рисунок 47 – Иконка в меню задач

3.9 Остановка обработчика ПК «АК СКЗИ»

Правый клик по иконке в меню задач вызовет меню приложения ПК «АК СКЗИ». Для завершения работы обработчика ПК «АК СКЗИ» нужно выбрать пункт «Выход» (Рисунок 48).

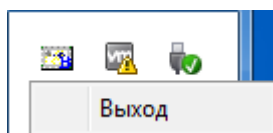


Рисунок 48 – Меню обработчика ПК «АК СКЗИ»

3.10 Обработка ошибок ПК «АК СКЗИ»

При возникновении не критичной ошибки при обработке обработчик ПК «АК СКЗИ» запишет отчет об ошибке в журнал и продолжит обработку. При возникновении одной из четырех критических ошибок:

- Ошибка чтения ключа реестра;
- Ошибка записи в журнал;
- Ошибка инициализации криптопрофиля;
- Ошибка поиска рабочего сертификата,

обработчик прекратит работу и вызовет окно с описанием ошибки (Рисунок 49).

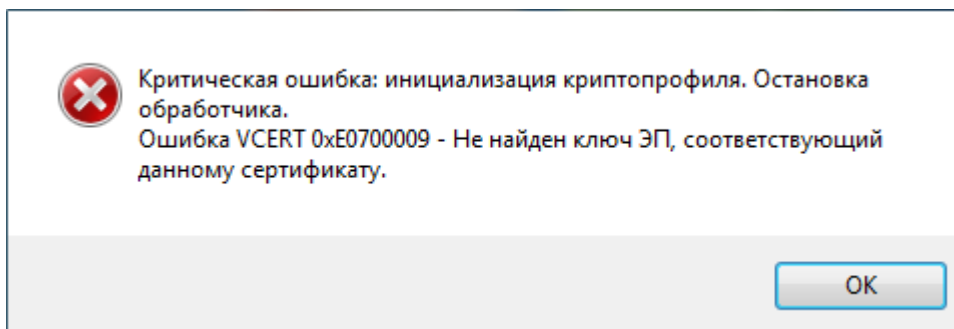


Рисунок 49 – Критическая ошибка обработчика ПК «АК СКЗИ»

Ошибка чтения ключа реестра может быть связана с повреждением данных в реестре. Ошибка записи в журнал может быть связана с повреждением каталога, выбранного как путь для записи журнала. Ошибки инициализации криптопрофиля и поиска рабочего сертификата могут быть связаны с некорректной работой или настройкой ПК «СКЗИ «Валидата CSP» версия 6» или ПК «Валидата Клиент» версия 4», установленных на данной машине.

Внимание! Использование клиентской и сервисной версий ПК «АК СКЗИ» на одной ЭВМ одновременно не рекомендуется. При использовании этих программ на одной машине следует удостовериться, что названия профилей, каталоги, в которых будет производиться обработка, и каталоги журналов не совпадают, иначе может произойти потеря данных.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

КЗИ	Криптографическая защита информации
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
ЭВМ	Электронно-вычислительная машина

ПЕРЕЧЕНЬ РИСУНКОВ

1	Интерфейс модуля конфигурации ПК «АК СКЗИ»	7
2	Выбор пути записи журнала	8
3	Настройка расширений для обрабатываемых файлов	8
4	Добавление дополнительного расширения	10
5	Удаление дополнительного расширения	10
6	Создание нового профиля	11
7	Добавление профиля справочника в список	12
8	Выбор профиля из списка профилей справочника	13
9	Переключение между настройками профилей справочников	14
10	Удаление профиля справочника из списка	17
11	Переключение профилей	18
12	Редактирование профиля	19
13	Удаление профиля	20
14	Создание нового правила	20
15	Создание новой маски правила	24
16	Редактирование маски правила	24
17	Удаление масок правила	25
18	Выбор сертификатов получателей	26
19	Окно фильтра владельцев сертификатов в сетевом справочнике	28
20	Сохранение группы сертификатов получателей	28
21	Добавление группы сертификатов получателей	29
22	Добавление сертификатов в список получателей	29
23	Удаление сертификатов из списка получателей	30
24	Настройка правила «Переместить»	30
25	Выбор формата архивации	32
26	Выбор типа создаваемой подписи	32
27	Дополнительные параметры функции «Переподписать»	33
28	Дополнительные параметры функции «Упаковать файлы»	34
29	Дополнительные параметры функции «Упаковать файлы»	35
30	Окно добавления списков подписантов	36
31	Создание списка подписантов	37
32	Изменение списка подписантов	38
33	Информация о списке	39
34	Удаление списков подписантов	39
35	Добавление описания к правилу	40
36	Копирование правила	40
37	Редактирование правила	41
38	Удаление правила	42
39	Временное отключение правила	42
40	Подробная информация о пункте правила	43
41	Сохранение правил профиля в файл	43
42	Добавление правил профиля из файла	44
43	Поиск правил по описанию	45
44	Сохранение внесенных изменений	45
45	Диалог с предложением сохранить изменения	46
46	Интерфейс обработчика ПК «АК СКЗИ»	46

47	Иконка в меню задач	46
48	Меню обработчика ПК «АК СКЗИ»	47
49	Критическая ошибка обработчика ПК «АК СКЗИ»	47

ПЕРЕЧЕНЬ ТАБЛИЦ

1	Настройки расширений для обрабатываемых файлов	9
2	Настройки профиля, привязанные к выбранному профилю справоч- ника	15
3	Общие настройки профиля ПК «АК СКЗИ»	16

[illegible][illegible]