СПЕКТР

МАРКЕР

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Версия документа: 3.4
Дата ревизии документа: 20.01.2024

Оглавление

1. Введение

1.1. Цель документа

Цель данного документа - описать возможности, предоставляемые системой “Спектр. Маркер” (далее Система).
Документ покрывает основные пользовательские и технические сценарии, а также элементы интерфейса, который предоставляет единую точку входа для управления системой.

1.2. Целевая аудитория

Документ предназначен для сотрудников отдела информационных технологий и служб информационной безопасности организации.

1.3. Термины, определения и сокращения

ПО	Программное обеспечение
Администратор системы	Сотрудник, обладающий учетной записью с административными привилегиями, отвечающий за настройку и поддержание в рабочем состоянии системы “Спектр”
Оператор системы	Сотрудник, занимающийся мониторингом событий доступа к хранилищам неструктурированных данных, их структуры, а также структуры организации, включающей права доступа.
Почтовый сервер	Сервер пересылки и хранения электронных почтовых сообщений
ОС	Операционная система - комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем
Браузер	Программное средство навигации и просмотра ресурсов сети интернет
ИТ / IT	Информационные технологии
ИБ	Информационная безопасность

2. Обзор

2.1. Назначение системы

Система “Спектр. Маркер” – это решение для эффективного управления и применения политик классификацией данных в рамках всей организации. Система позволяет быстро настраивать и устанавливать метки на различные документы и почтовые сообщения, а также применять различные правила и ограничения по использованию данных.

2.2. Функциональные возможности

Система «Спектр. Маркер»:

- Предоставляет возможность создания и настройки меток документов согласно принятой в организации политики;

- Предоставляет возможность создания и настройки правил, ограничивающих действия сотрудников организации с промаркированными данными:
    - Запрет или предупреждение об отправке по почте документов без метки;
    - Запрет или предупреждение об отправке по почте документов с определенной метки на внешние / недоверенные почтовые адреса;
    - Запрет или предупреждение об изменении текущей метки документа

- Фиксирует все действия с метками документов (Чтение, Создание, Изменение, Удаление);
- Фиксирует действия с письмами содержащие метку (Создание / Изменение / Удаление метки при сохранении письма, Отправка письма, Добавление неподтвержденных получателей)

2.3. Схема взаимодействия модулей системы

Система “Спектр. Маркер” состоит из двух логических частей:

- серверная часть - набор модулей, обеспечивающих логику работы и управления, включая базу данных;
- клиентская часть - приложение, устанавливаемое непосредственно на рабочие станции сотрудников организации, добавляющее функциональность по по просмотру / установке меток и применения политик по работе с данными.

2.3.1. Матрица сетевого взаимодействия

ИЗ → **----------** **В ↓**	**Сервер “Спектр. Маркер”**	**Рабочее место администратора “Спектр.Маркер”**	**Рабочее место сотрудников организации**
Сервер “Спектр. Маркер”		TCP:443 TCP:22	TCP:7100 TCP:7200
Рабочее место администратора “Спектр.Маркер”			
Рабочее место сотрудников организации			
MS ActiveDirectory	TCP:389 (LDAP) TCP:636 (LDAPS)		
MS Exchange или др.почтовый сервер	TCP:25 (SMTP)		

3. Установка системы

Установка системы “Спектр. Маркер” состоит из следующих действий:

- Установка операционной системы
- Настройка сетевого адреса и DNS
- Установка серверного ПО “Спектр”
- Установка агентского ПО “Спектр”

3.1 Установка операционной системы

ПО “Спектр” может функционировать в следующих операционных системах:

- Ubuntu Server 20.04, 22.04

- CentOS\RHEL\OracleLinux 7.9
- Astra Linux релиз Orel 1.7
- RedOS 7.3 Murom

ПО “Спектр.Маркер” может быть установлено на ОС, расположенных на виртуальных машинах под управлением гипервизоров:

- VmWare ESXi,
- MS Hyper-V,
- KVM\QEMU-based гипервизоры

Выбор операционной системы, в которой будет функционировать серверное ПО “Спектр.Маркер” зависит от принятых в организации стандартов и политик.

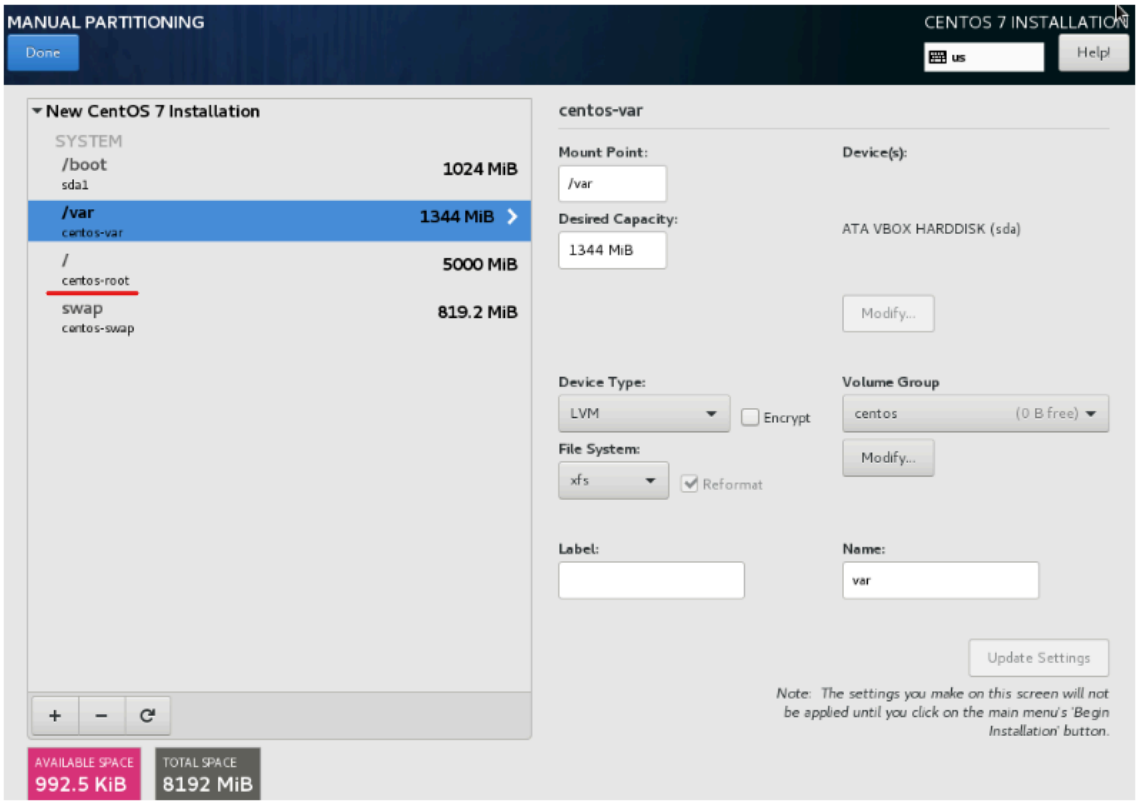
Установку ОС следует производить согласно стандартным инструкциям, прилагающимся к каждой из вышеперечисленных ОС и доступным по следующим ссылкам:

- Ubuntu Server: https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-server#0
- CentOS: https://docs.centos.org/en-US/centos/install-guide/
- Red Hat Enterprise Linux 7: https://access.redhat.com/documentation/ru-ru/red_hat_enterprise_linux/7/html/installation_guide/index
- Astra Linux Орел 1.7.3: https://wiki.astralinux.ru/pages/viewpage.action?pageId=37290417
- RedOS 7.3 Murom: https://redos.red-soft.ru/base/manual/redos-manual/red-os-installation/start-install/

Важно: при установке операционной системы в целях безопасности обязательно назначайте сложный (состоящий минимум из 8 символов, содержащий минимум одну цифру и минимум один спец. символ такой как @, #, $) пароль для пользователя root.

3.1.1 Рекомендации по разбивке жесткого диска

Для наиболее рационального использования жесткого диска рекомендуется проводить его первоначальную разбивку таким образом, чтобы в корневом разделе “/” было минимум 40 Гб доступного пространства, а в разделе “/var” не менее 70% от общего объема диска.
Если “/var” не выделяется в отдельный раздел (при этом физически будет располагаться в корневом разделе), размер корневого раздела должен рассчитываться как 70% от объема общего доступного места плюс минимум 40Гб.



Настройками разбивки диска при инсталляции ОС CentOs

3.1.2 Настройка сетевого адреса и DNS

Инструкция по настройка сетевого адреса и DNS будет приведена на примере ОС Ubuntu Server.
Для настройки статического IP-адреса зайдите в консоль ОС и выполните команду

```
ifconfig -a
```

для просмотра всех доступных сетевых интерфейсов:

```
root@democp:/etc/netplan# ifconfig -a
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 94.250.254.105  netmask 255.255.255.255  broadcast 94.250.254.105
        inet6 fe80::5054:ff:fec3:c736  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:c3:c7:36  txqueuelen 1000  (Ethernet)
        RX packets 60433522  bytes 55580494752 (55.5 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59801104  bytes 8870034232 (8.8 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 34320447  bytes 46678318464 (46.6 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34320447  bytes 46678318464 (46.6 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Просмотр доступных сетевых интерфейсов

Далее необходимо приступить к редактированию конфигурационного файла netplan, выполнив команду:

```
sudo nano /etc/netplan/*.yaml
```

Откроется редактор nano, необходимо отредактировать конфигурационный файл следующим образом:

```
network:
  renderer: networkd
  ethernets:
    ens3:
      addresses: [192.168.3.110/24]
      gateway4: 192.168.1.1
      dhcp4: no
      dhcp6: no
      nameservers:
       addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

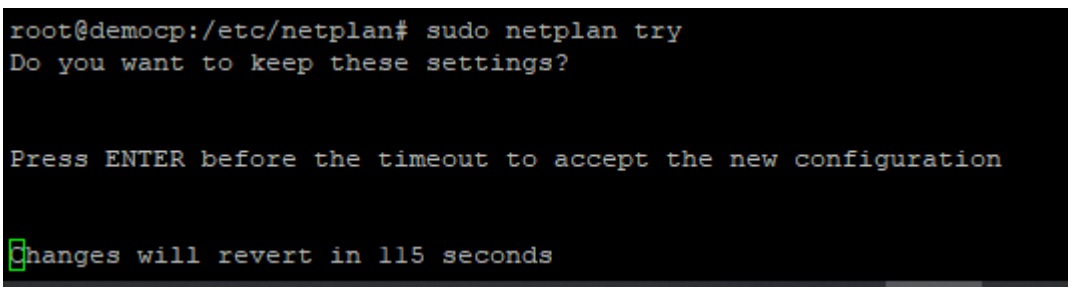
Где

ens3 - имя сетевого интерфейса
addresses: [192.168.3.110] - статический IP-адрес, присвоенный серверу
nameservers: - блок с настройками DNS.
addresses: [8.8.8.8,8.8.4.4] - IP-адреса DNS-серверов, можно указать несколько через запятую.

Для сохранения изменений и выхода из редактора нажмите “Ctrl+o” и затем “Enter”. После внесений изменений в конфигурационный файл и его сохранения необходимо проверить конфигурацию на наличие ошибок и в случае их отсутствия применить изменения. Для этого в консоли выполните команду:

```
sudo netplan try
```

Если ошибок нет, то вы получите сообщение: "Вы хотите сохранить эти настройки?" Нажмите ENTER:



Выполнение команды “sudo netplan try”

3.2 Установка серверного ПО “Спектр.Маркер”

Для установки серверного ПО “Спектр.Маркер” необходимо:

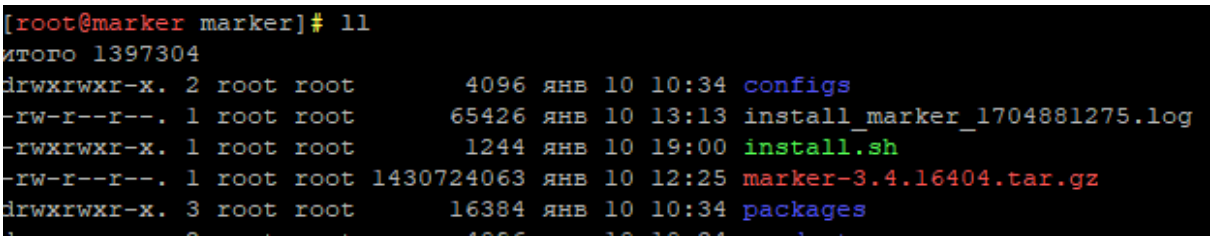
1. скопировать заархивированный установочный пакет marker-x.x.tar.gz на подготовленный сервер (Для этого можно использовать любой sFTP-клиент, например, WinCSP) в заранее подготовленную пустую папку.
2. в консоли сервера перейти в папку со скопированным архивом и выполнить команду по разархивированию:

```
tar -xzf marker-x.x.tar.gz
```

3. запустить скрипт автоматической установки и конфигурирования ПО “Спектр.Маркер”:

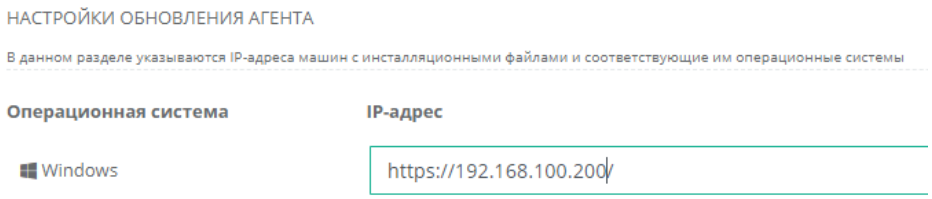
```
sudo ./install.sh
```

Далее выбрать язык процесса инсталляции и подтверждать дальнейшие действия в этом процессе.
После завершения установки ПО на экране будет выведено соответствующее сообщение.
Для проверки корректности установки нужно проверить логи инсталляции, которые сохраняются с именем install_marker_*.log в той же директории, что и запускаемый скрипт install.sh.



Лог инсталляции

Далее необходимо проверить доступ к модулю управления системы через веб-браузер. Для этого в адресной строке введите IP-адрес сервера, на который производилась установка ПО “Спектр.Маркер”. Должна отобразится форма авторизации в системе.
Дальнейшие действия:
- “Системные настройки” - “Модуль управления агентами” - заполнить адрес\порт для получения событий от агентов (адрес сервера “Спектр.Маркер”).
- “Системные настройки” - “Настройки агента маркера” - заполнить адрес, на который агенты будут обращаться за обновлениями:



4. Работа с модулем управления системой

4.1. Программное обеспечение для работы администратора системы

Графический интерфейс администратора системы “Спектр. Маркер” выполнен в виде веб-приложения. Доступ к интерфейсу осуществляется с использованием одного из следующих веб-браузеров:

- Google Chrome версии 60.0.3112 и выше;
- Яндекс.Браузер версии 17.6.1 и выше
- Mozilla Firefox версии 52 и выше;
- Microsoft Edge;

Операционная система, на которой запускается веб-браузер, может быть любой из поддерживаемых конкретной версией браузера.

4.2. Обзор интерфейса системы

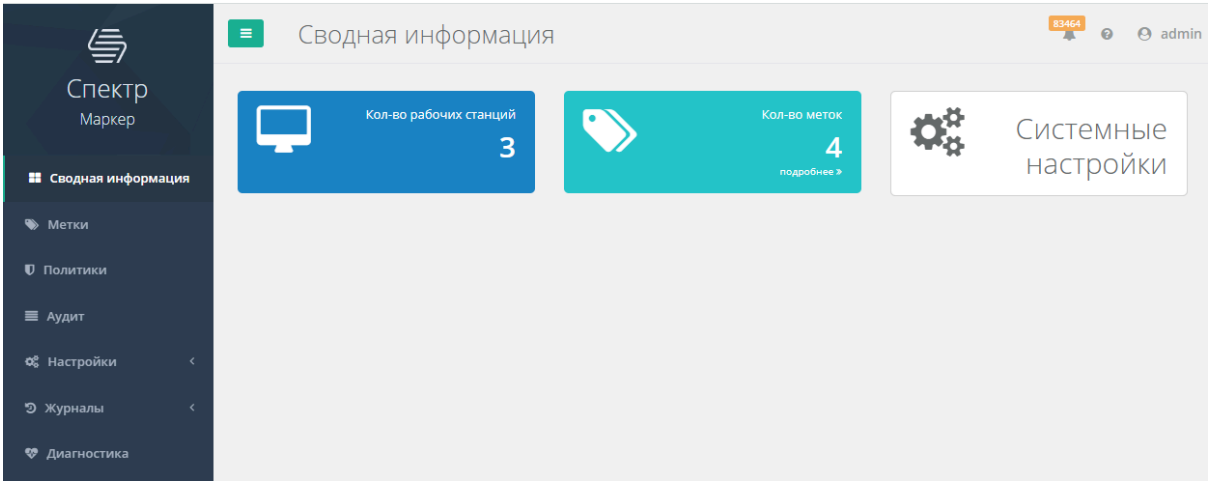


Рис.: Стартовая страница интерфейса

Интерфейс системы “Спектр. Портал заявок” состоит из нескольких разделов, каждый из которых предлагает определенный набор функций.
В левой части интерфейса располагается меню

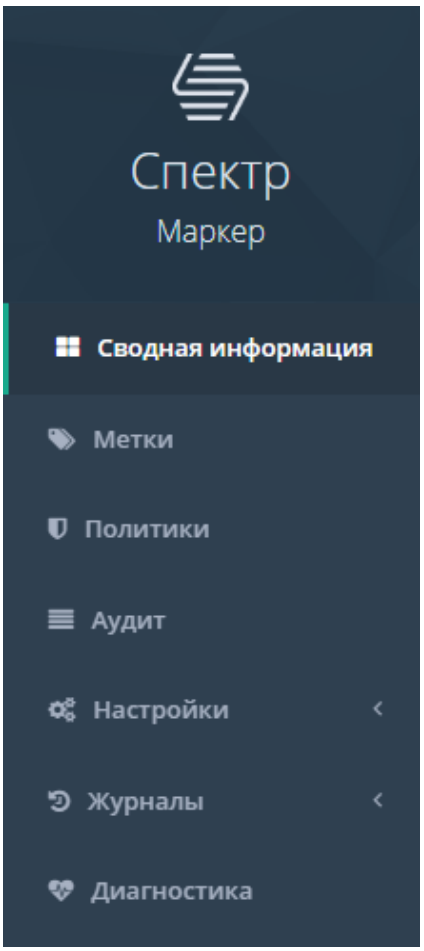


Рис.: Главное меню интерфейса

с ссылками на следующие разделы:

- Сводная информация - это стартовый экран администратора системы. Содержит информацию о функционировании системы, а также блоки с наиболее важной статистической информацией и ссылки для быстрых переходов в другие разделы интерфейса.

- Метки - данный раздел служит для настройки меток, которые потом будут отображаться в документах и письмах.

- Политики - данный раздел служит для настройки политик, настроенные политики будут ограничивать/предупреждать действия пользователей с документами, например, ограничение отправки письма с конфиденциальным вложением, и.д.

- Аудит - раздел, в котором отображаются зафиксированные события аудита в табличном представлении, с различными фильтрами, и детализацией по каждому событию

- Настройки - состоит из нескольких подразделов, предоставляющих функционал создания и управления учетными записями пользователей системы, настройки

интеграции системы с другими системами (почтовый сервер, контроллер домена) и др.

- Журналы - раздел для отображения системных событий и действий пользователей системы.

- Диагностика - раздел, доступный только администраторам системы. Отображает данные о текущих параметрах функционирования, внутренние метрики и другую диагностическую информацию.

В центральной части интерфейса располагаются данные и элементы управления, соответствующие выбранному разделу.

В правом верхнем углу интерфейса располагаются:
- Количество сообщений в системном журнале, на которые нужно обратить внимание оператору системы;
- Ссылки на документацию и описание системы;
- Кнопка выхода из системы (процедура деавторизации) и смены пароля

Рис.: Элементы в правом верхнем углу интерфейса

4.3. Работа с системой

4.3.1. Авторизация пользователя

Доступ к интерфейсу системы предоставляется только авторизованным пользователям. Для прохождения процедуры авторизации необходимо:

- Открыть веб-интерфейс Системы в вашем браузере (https://<IP-address>, где <IP-address> - IP-адрес, назначенный серверу “Спектр. Маркер” при установке)
- Заполнить поля “логин” и “пароль”, также доступна доменная авторизация, данный функционал будет описан подробнее в разделе “Управление пользователями”
- Нажать “Вход”

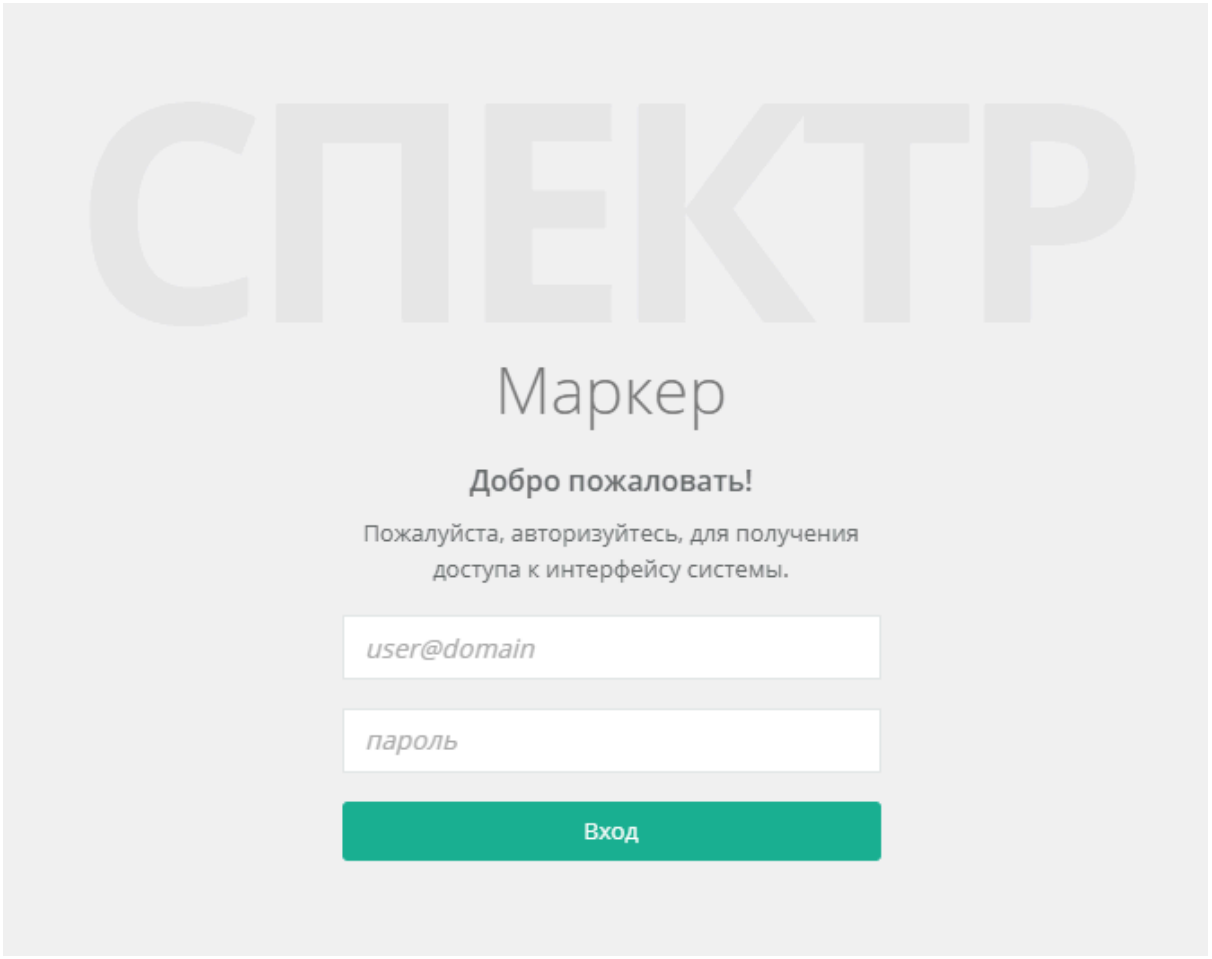


Рис.: Экран авторизации в системе

Если логин и пароль введены корректно, то перед вами откроется интерфейс Системы. Если нет - то будет отображено сообщение с ошибкой.

Для выхода из системы (процедуры деавторизации или logout) достаточно нажать на кнопку “Выйти”, которая доступна в выпадающем меню при нажатии на логин текущего пользователя в правом верхнем углу интерфейса:

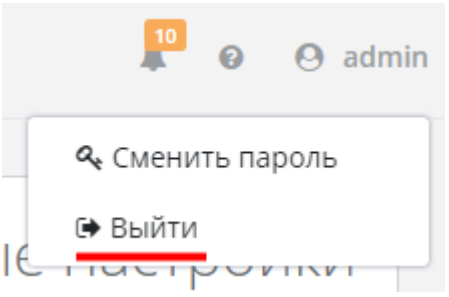


Рис.: Кнопка выхода из системы

Также процесс деавторизации (logout) по умолчанию производится автоматически, если пользователь системы неактивен в течение заданного в настройках системы промежутка времени.

4.3.2. Сводная информация

Раздел “Сводная информация” состоит из нескольких блоков-виджетов со сводной информацией и ссылкой на соответствующий раздел.

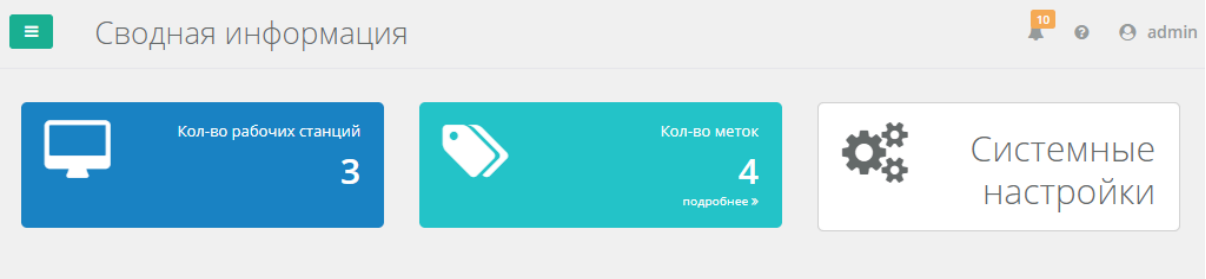


Рис.: Виджеты раздела “Сводная информация”

- Кол-во рабочих станций - кол-во рабочих станций (компьютеров), на которых установлено агентское ПО “Маркер”
- Кол-во меток - кол-во меток первого уровня, которые настроены в системе.
- Системные настройки - быстрый переход в раздел “Системные настройки” системы.

4.3.3. Метки

В раздел “Метки” можно перейти из главного меню, выбрав пункт “Метки”. Этот раздел содержит все настроенные метки. Слева располагается список всех меток первого уровня, справа окно с детальной информацией метки и возможностью ее редактирования. Пример изображен на рисунке ниже.

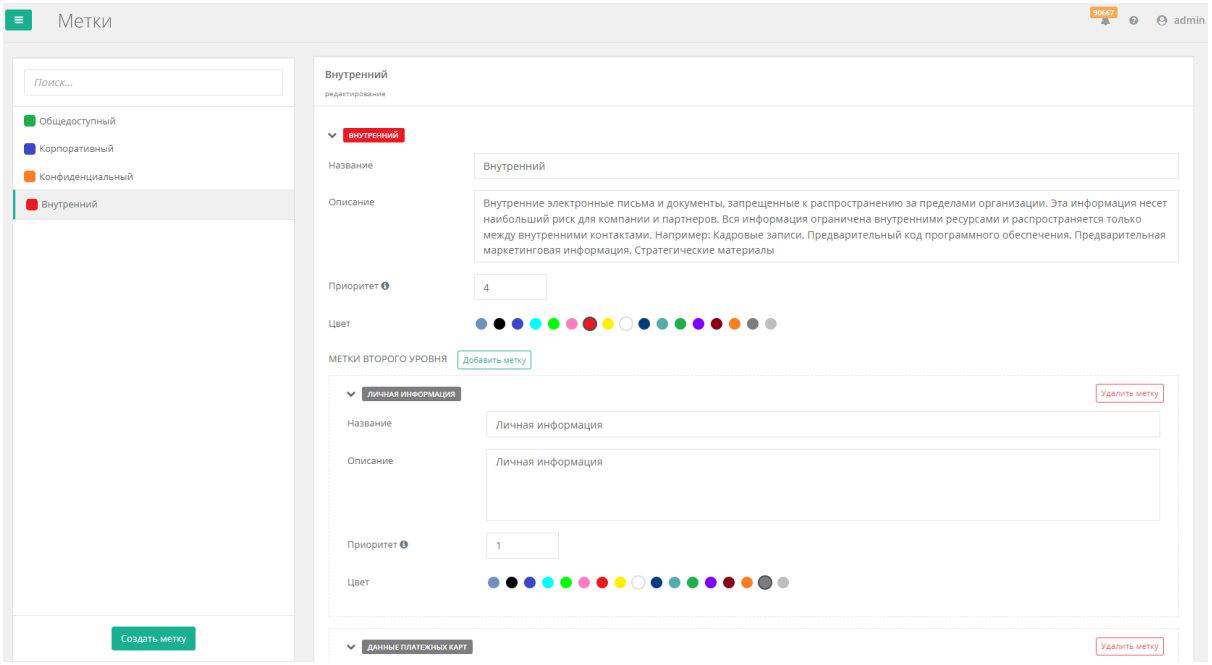


Рис.: Раздел “Метки”

Для редактирования метки необходимо выбрать ее в списке слева. Изменить название, описание, приоритет и цвет. Также к метке можно добавить метки второго уровня, нажав на кнопку “Добавить метку”, или удалить, нажав, на кнопку “Удалить метку”. Метки второго уровня также содержат следующие поля: название, описание, приоритет и цвет.

После того, как вся информация о метке и ее метках второго уровня заполнена, необходимо нажать на кнопку “Сохранить” внизу экрана. Для создания новой метки необходимо нажать на кнопку “Создать метку”, для отмены изменений, нажать на кнопку “Отмена”

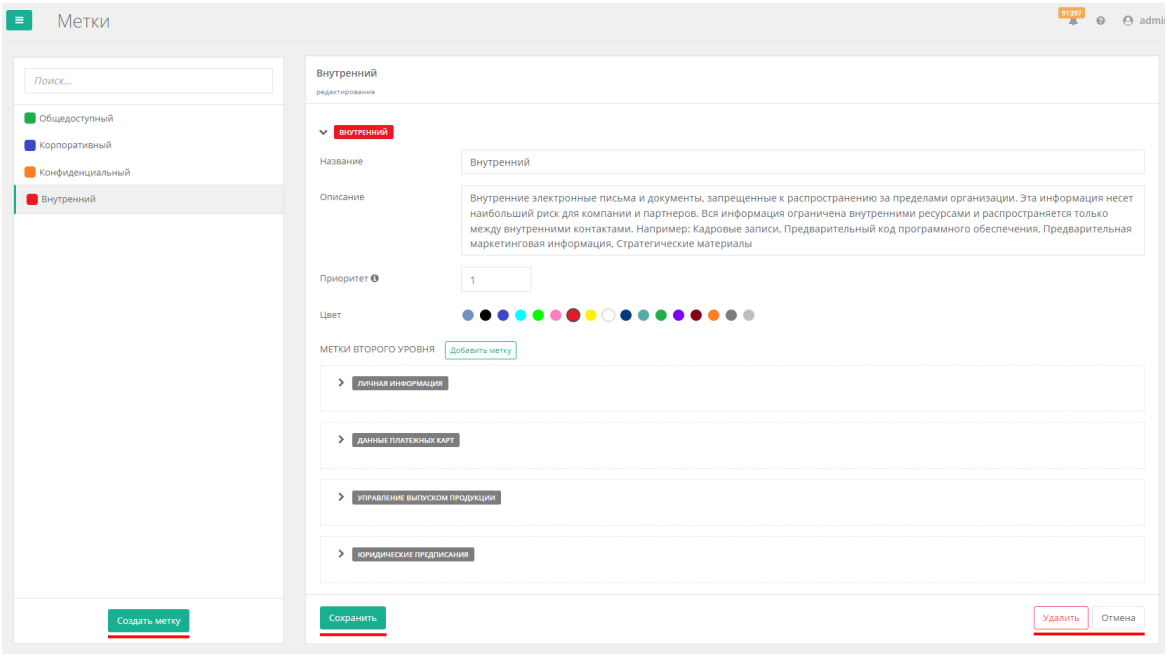


Рис.: Редактирование информации метки

Для удаления метки необходимо нажать на кнопку удалить, после этого появится окно подтверждения удаления метки, где необходимо подтвердить действие, см. рис. ниже:

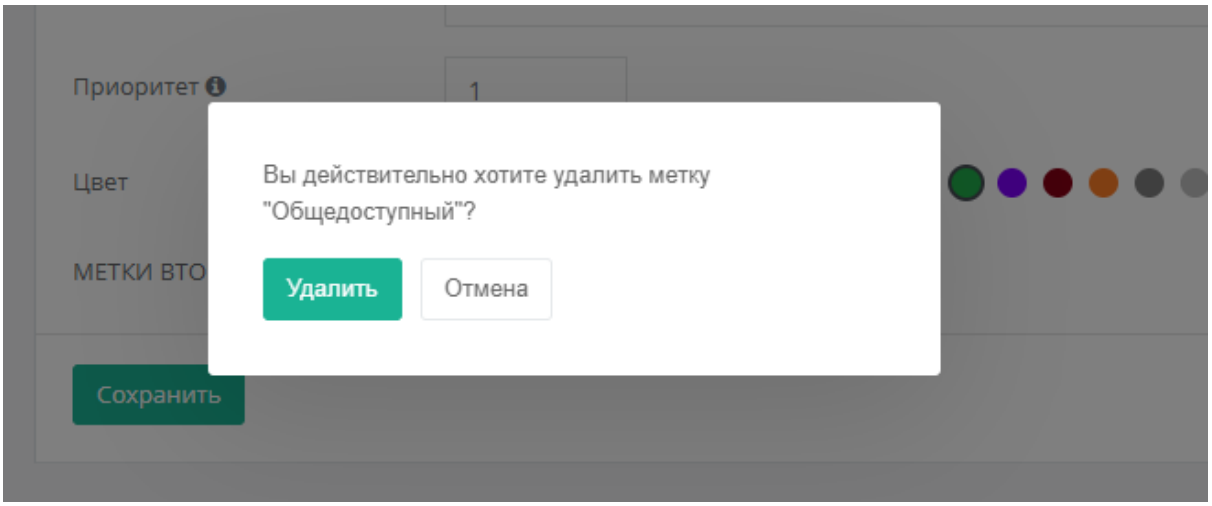


Рис.: Окно подтверждения удаления метки

4.3.4. Политики

В раздел “Политики” можно перейти из главного меню пункт “Политики”. Этот раздел содержит все настроенные политики. Слева располагается список всех политик, справа окно с детальной информацией о политике, с возможностью ее редактирования. Пример изображен на рисунке ниже.

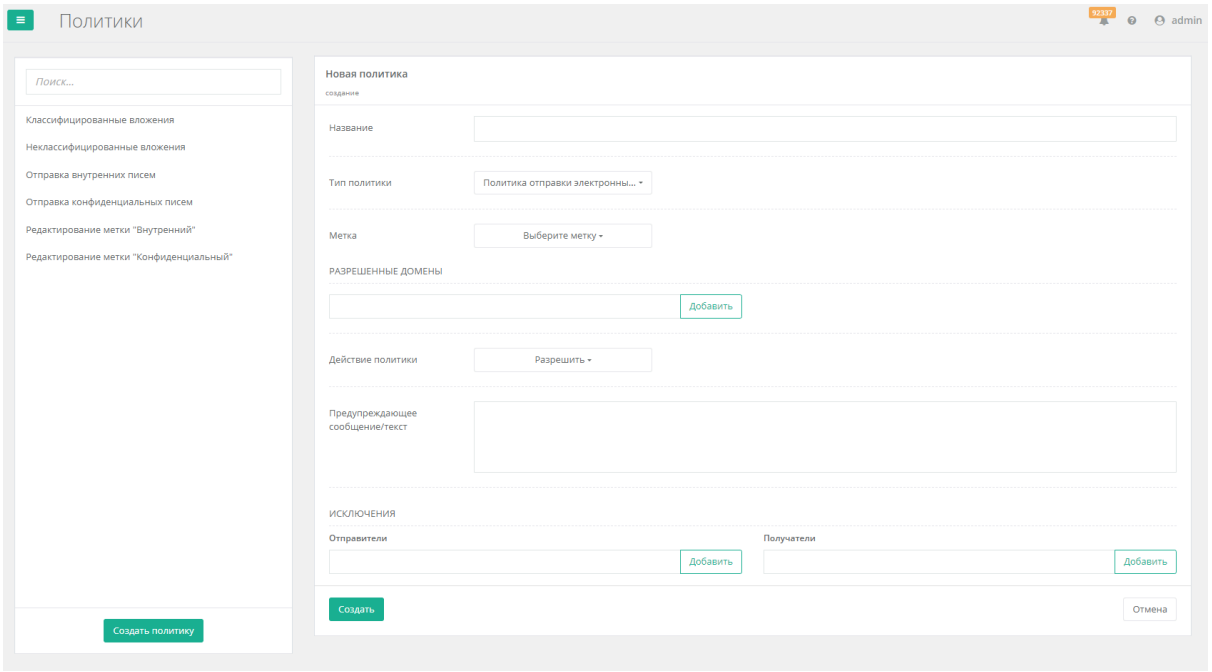


Рис.: Раздел “Политики”

Существует 4 вида политик:

- Политика отправки электронных писем - политика с этим типом задает правила для определенной метки: разрешить, предупредить пользователя или запретить отправлять письма с выбранной меткой
- Политика неклассифицированных вложений - задает правила для неклассифицированных вложений
- Политика классифицированных вложений - задает правила для классифицированных вложений
- Политика ограничений действий с метками - политика с этим типом задает ограничения/разрешения для работы с определенной меткой.

Политика неклассифицированных/классифицированных вложений являются глобальными и настраиваются в единственном экземпляре для всех меток.

Для каждого из типов политик существуют определенные настройки.

Для политики отправки электронных писем, необходимо задать название политики, выбрать метку, задать список разрешенных доменов, выбрать действие, задать предупреждающее сообщение, и при необходимости задать списки исключений отправителей и получателей, для кого данная политика не будет распространяться см. рис. ниже:

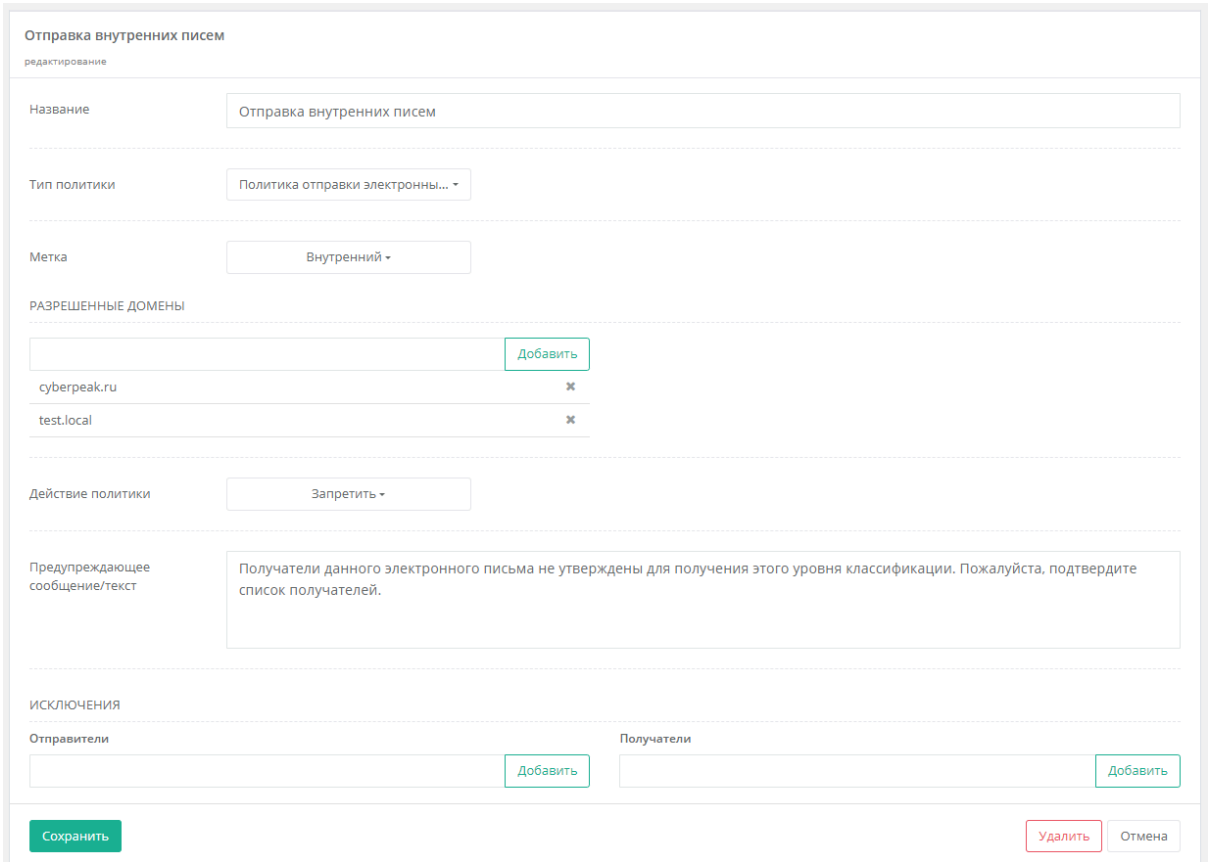


Рис.: Политика отправки электронных писем

Для политик неклассифицированных/классифицированных вложений необходимо задать название политики, действие и предупреждающее сообщение, см. рис. ниже:

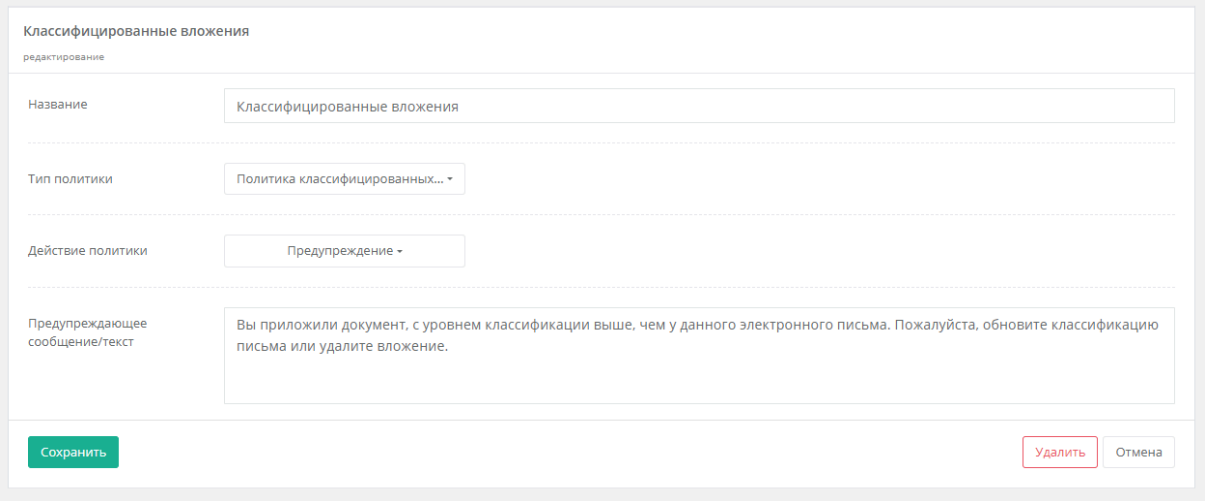


Рис.: Политики неклассифицированных/классифицированных вложений

Для политики ограничений действий с метками необходимо задать название политики, выбрать метку, выбрать кому разрешены действия с меткой (автор, учетные записи, и учетные записи которые входят в определенные группы безопасности), выбрать действия, которые разрешены, и предупреждающее сообщение, см. рис. ниже:

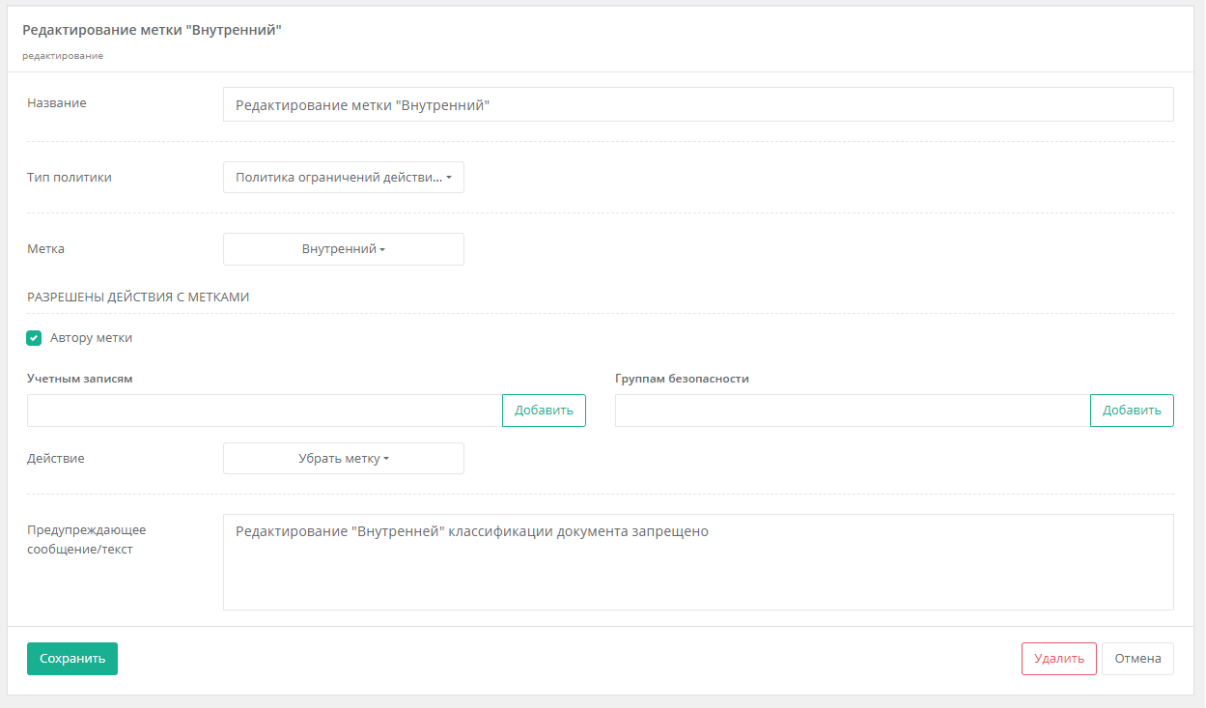


Рис.: Политика ограничений действий с метками

После внесения всех изменений политику необходимо применить нажатием на кнопку “Сохранить”, для удаления политики, необходимо нажать на кнопку “Удалить” и подтвердить удаление политики в подтверждающем модальном окне, см. рис. ниже:

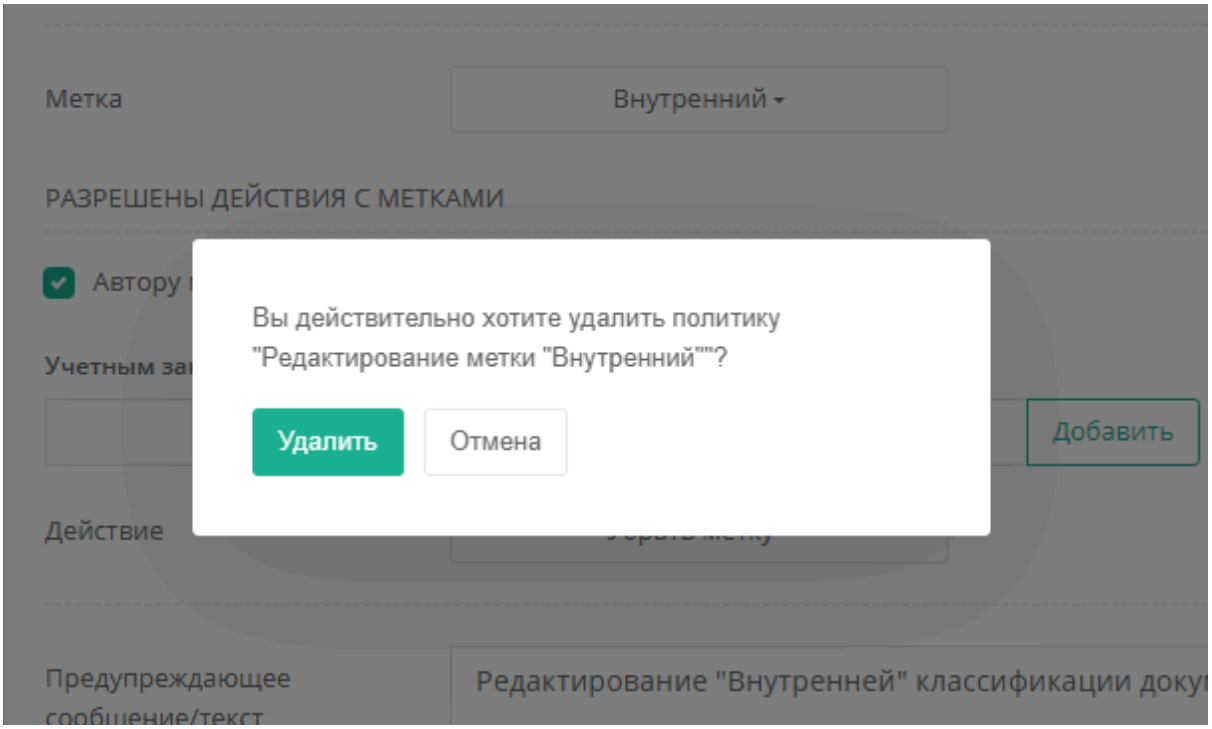


Рис.: Окно подтверждения удаления политики

4.3.5. Аудит

В раздел “Аудит” можно перейти из главного меню пункт “Аудит”. Этот раздел содержит список всех событий с документами и письмами в табличном виде. Для удобства поиска событий, в верхней части экрана расположены различные фильтры. Пример изображен на рисунке ниже.

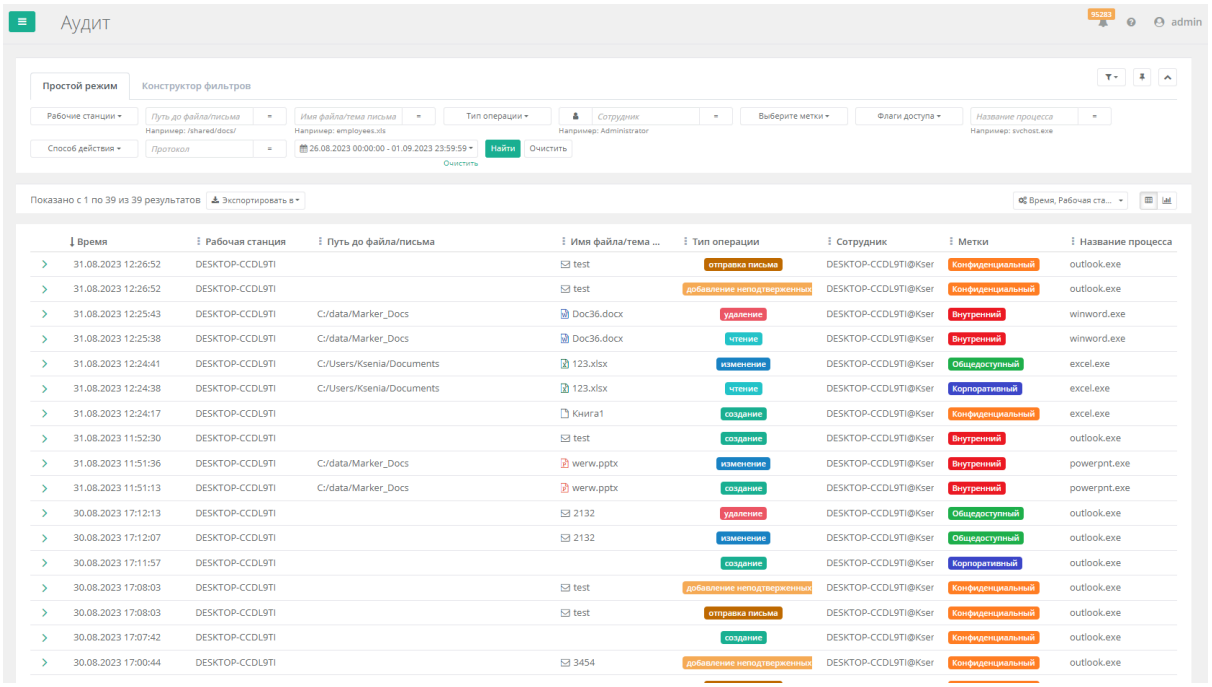


Рис.: Раздел “Аудит”

По каждому событию можно посмотреть его детализацию, нажатием на иконку галки напротив события, см. рис. ниже:

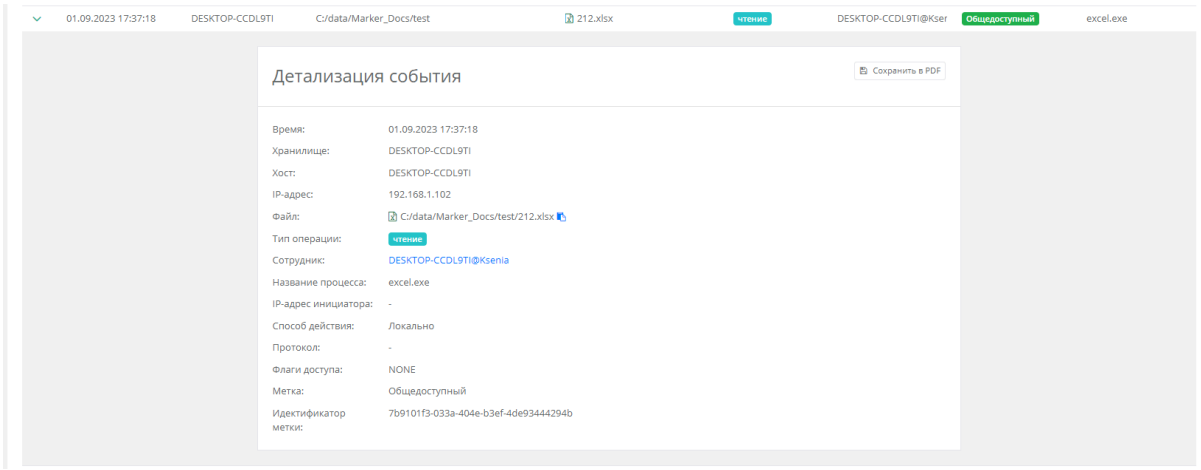


Рис.: Раздел “Аудит”

4.3.6. Управление настройками системы

Перейти в данный раздел можно в главном меню в разделе “Настройки->Системные настройки” блок “Продвинутые настройки системы”. В блоке “Продвинутые настройки системы” можно настроить:

- Локализацию веб интерфейса системы “Спектр. Маркер”
- Дополнительные настройки веб консоли.
- Настройки отображения меток
- Настройки агента маркера

При нажатии на пункт “Настройки локализации” развернется блок с выбором языка веб интерфейса, доступны два языка:

- Русский
- Английский

После выбора языка, необходимо нажать кнопку “Сохранить”, см. пример ниже:

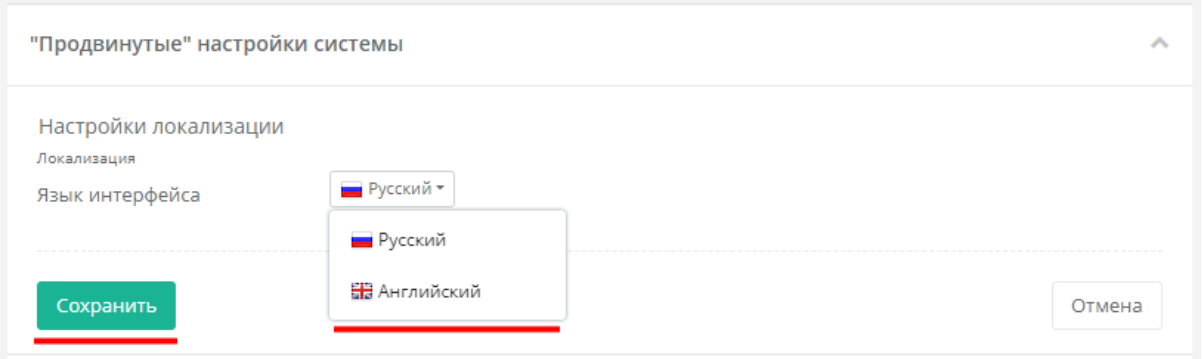


Рис.: Локализация веб интерфейса

Дополнительные настройки веб консоли включают в себя:

- Время неактивности - это время неактивности пользователя по истечении которого, сеанс работы с системой “Спектр. Маркер” закончится
- Парольная политика - это набор правил по составлению и сложности пароля

После внесения изменений необходимо нажать кнопку “Сохранить”, см. пример ниже:

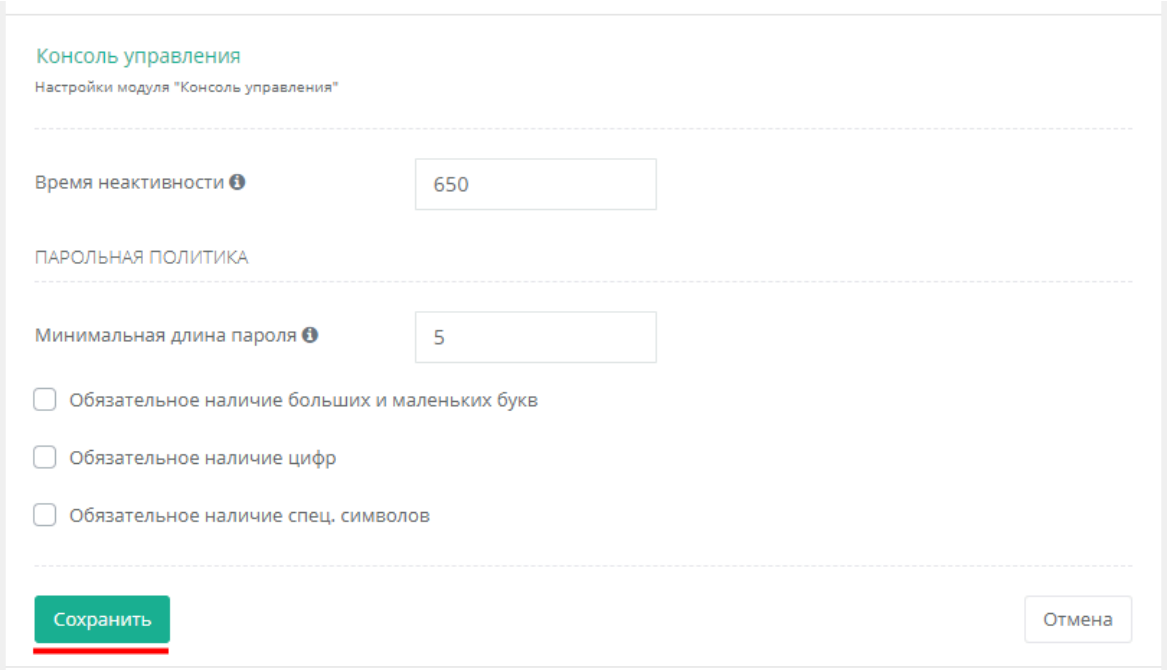


Рис.: Дополнительные настройки консоли управления

В настройках отображения меток можно изменить позиционирование меток, т.е. отображение меток в верхнем или нижнем колонтитуле, а также выравнивание по горизонтали: слева, справа и по центру. Также редактируется размер шрифта, цвет шрифта, можно загрузить картинку для метки. После внесенных изменений доступен предпросмотр отображения метки, см. на рис. ниже:

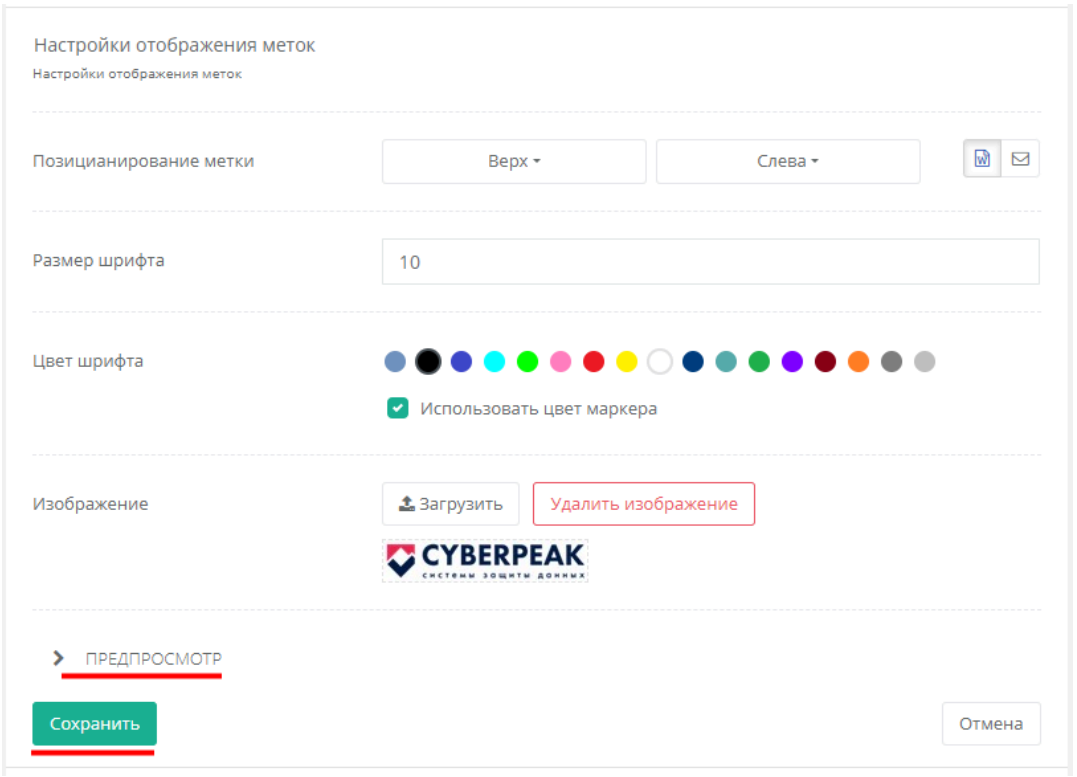


Рис.: Настройки отображения меток

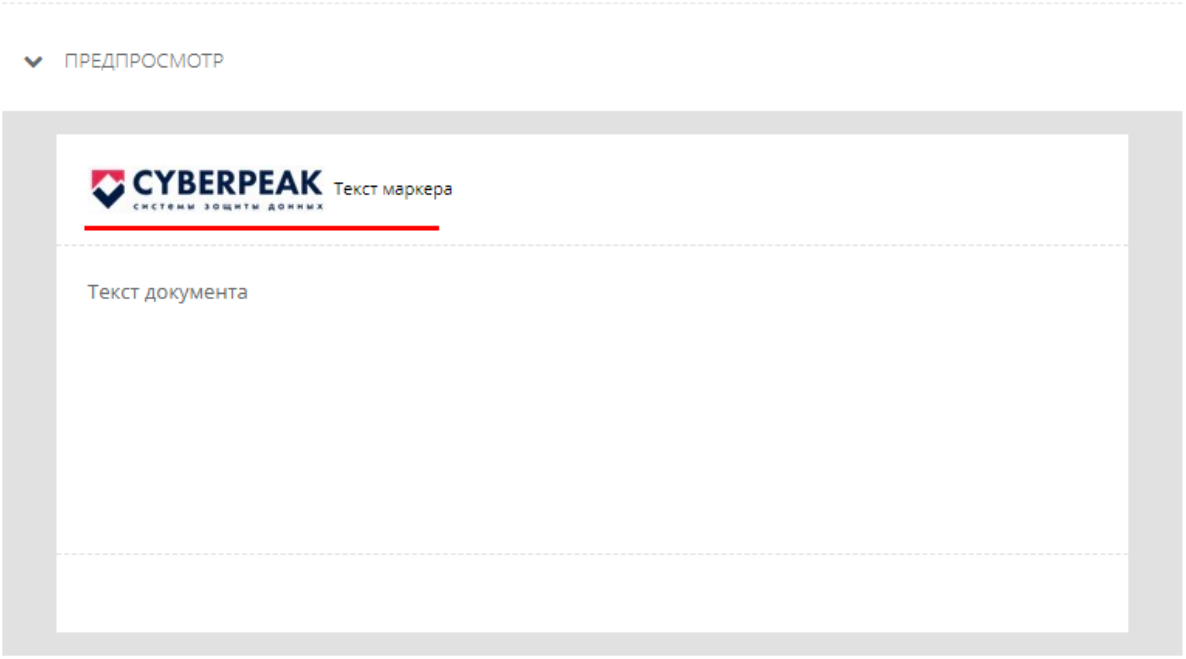


Рис.: Предпросмотр отображения меток

Существует два варианта настроек отображения меток:

- для документов
- для писем

Переключение между двумя режимами происходит нажатием на кнопку документа или письма, см. рис. ниже:

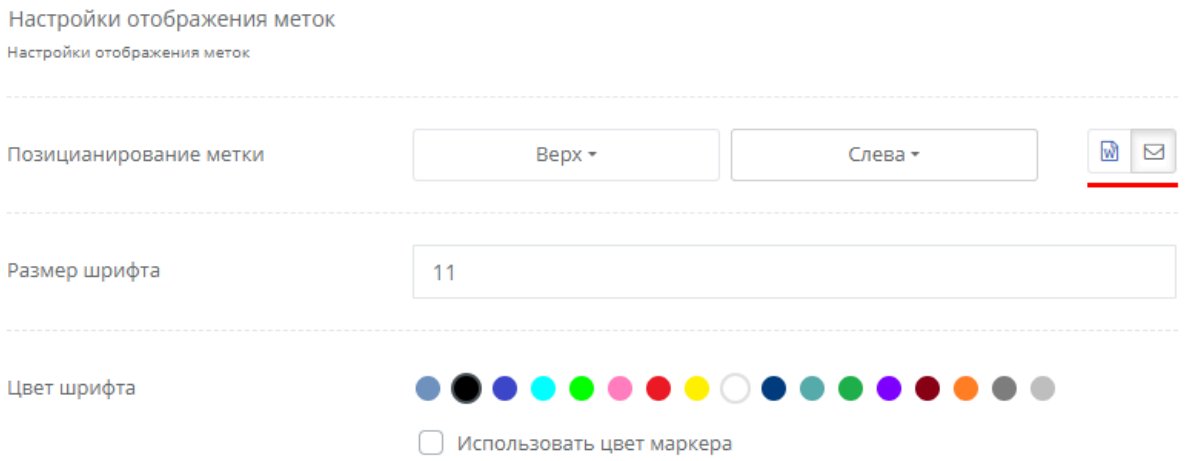


Рис.: Два режима настроек отображения меток

В настройках агента маркера можно задать таймаут агента, по умолчанию он равен 60 сек., см. рис. ниже.

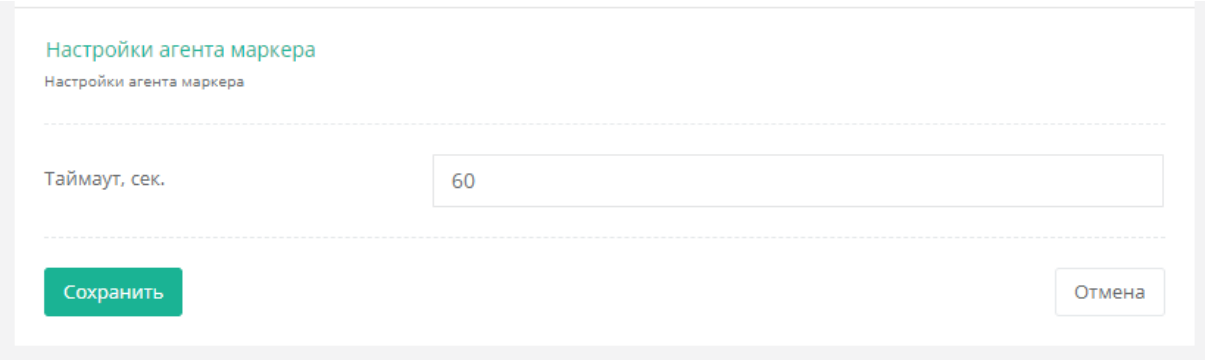


Рис.: Таймаут агента маркера

4.3.7. Синхронизация с контроллером домена

Для настройки синхронизации с MS Active Directory или другим LDAP-сервером перейдите в раздел “Настройки->“Системные настройки” в блок “Настройки синхронизации с LDAP” и заполните форму “Новый сервер LDAP”, учетная запись для синхронизации должна обладать правами чтения данных в Active Directory.

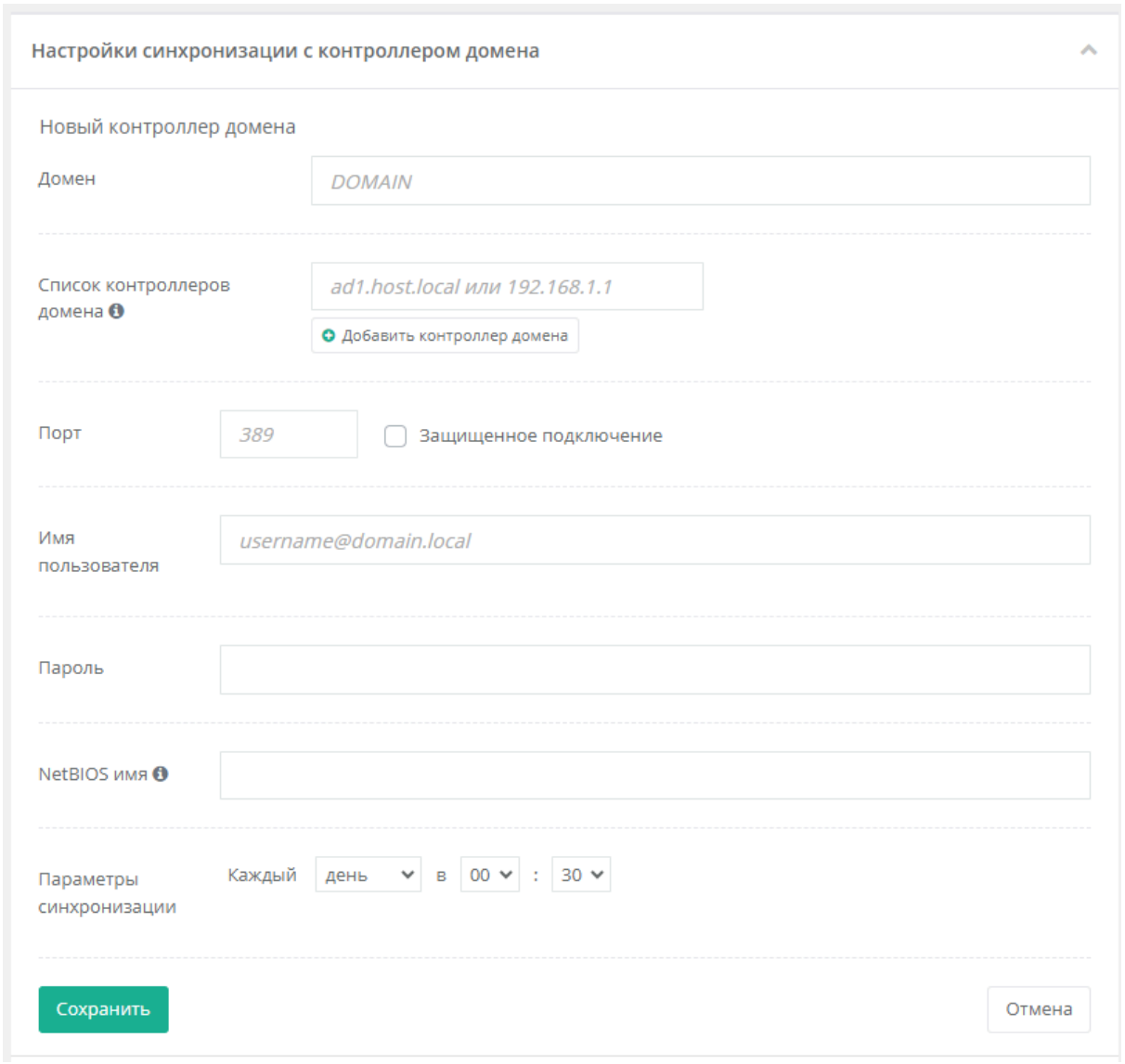


Рис.: Синхронизация с контроллером домена

После синхронизации с LDAP сервером, появится возможность добавлять доменных пользователей в систему “Спектр. Маркер” для доменной авторизации.

4.3.8. Настройка отправки почтовых сообщений

Раздел настройки синхронизации с контроллером домена доступен только администраторам системы “Спектр. Маркер”. Для настройки параметров отправки почтовых уведомлений системой перейдите в раздел “Настройки->Системные настройки” в блок “Настройки SMTP” и заполните соответствующую форму, указав в качестве имени пользователя и пароля данные учетной записи, имеющей права доступа на отправку почтовых сообщений.

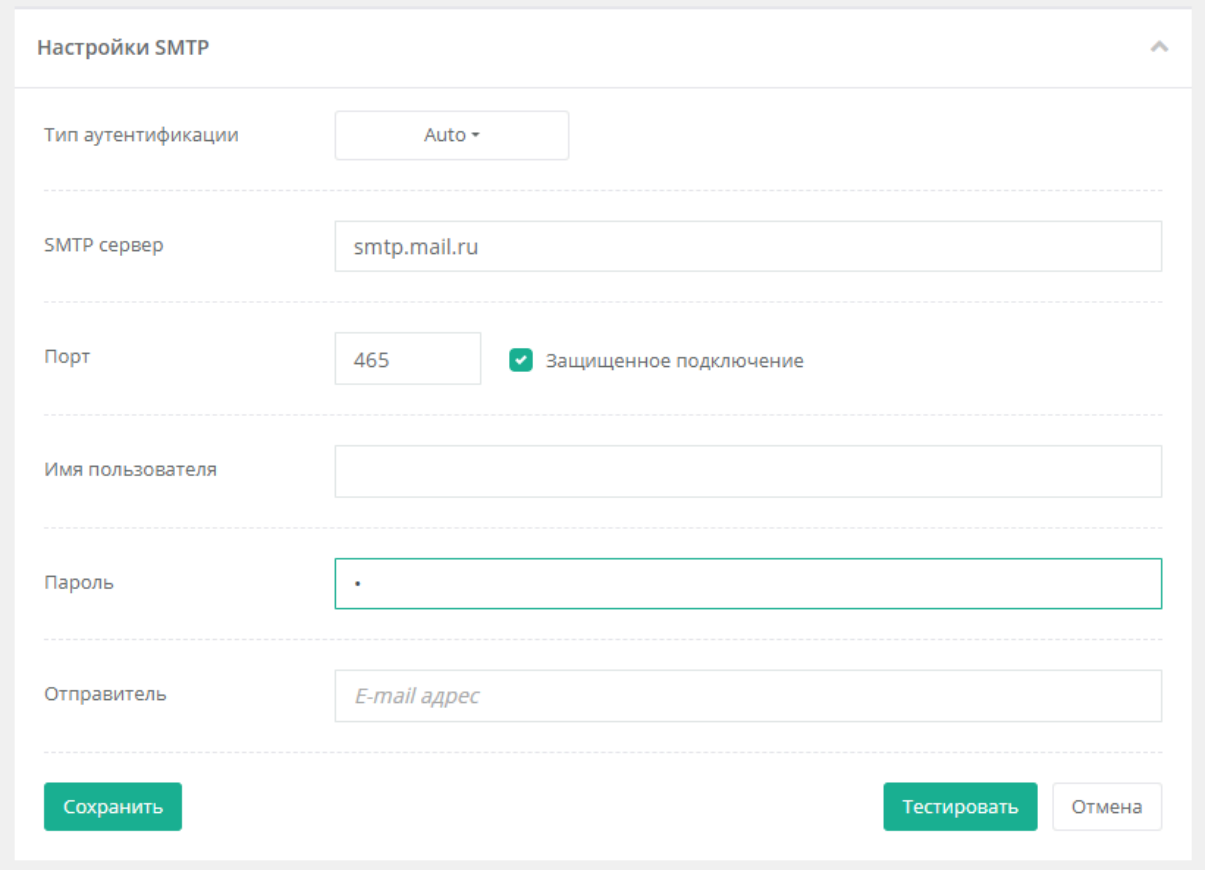


Рис.: Настройка отправки почтовых сообщений

Чтобы убедиться, в корректности функционирования отправки почтовых сообщений, нужно нажать на кнопку “Тестировать”, ввести свой e-mail и нажать на кнопку “Отправить”. Если все параметры указаны верно, на ваш почтовый ящик придет тестовой письмо.

4.3.9. Управление пользователями

Система “Спектр. Маркер” предоставляет возможность создания пользователей как с внутренней авторизацией так и авторизацией через Active Directory используя свои доменные учетные записи.

Перейти в раздел “Управление пользователями” можно в главном меню в разделе “Настройки->Управление пользователями”.

Список пользователей представлен в табличном виде, как на изображении ниже.

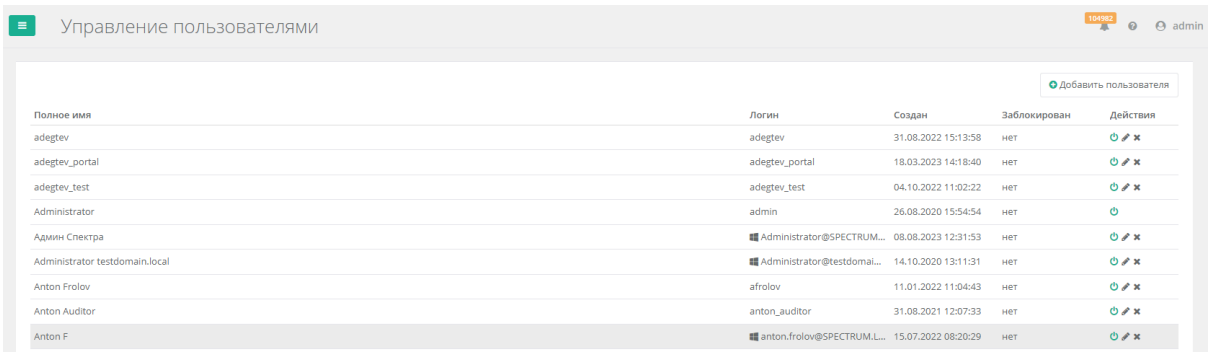


Рис.: Управление пользователями

Для того, чтобы добавить пользователя нужно нажать на кнопку “Добавить пользователя”, в появившемся модальном окне ввести, полное имя пользователя, логин, пароль, подтверждение пароля и нажать кнопку “Создать”, см. пример ниже:

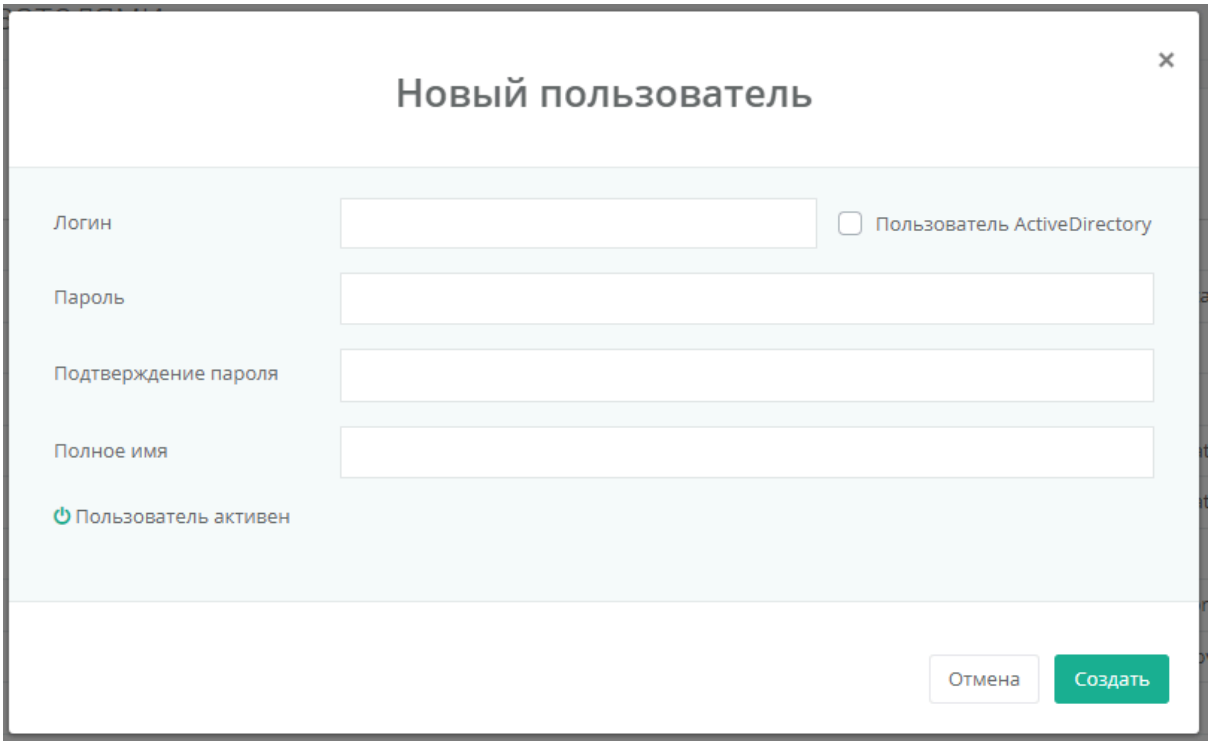


Рис.: Создание пользователя

В случае создания доменного пользователя, необходимо выбрать чекбокс “Пользователь ActiveDirectory” ввести логин пользователя используя авто подсказку, как на рис. ниже:

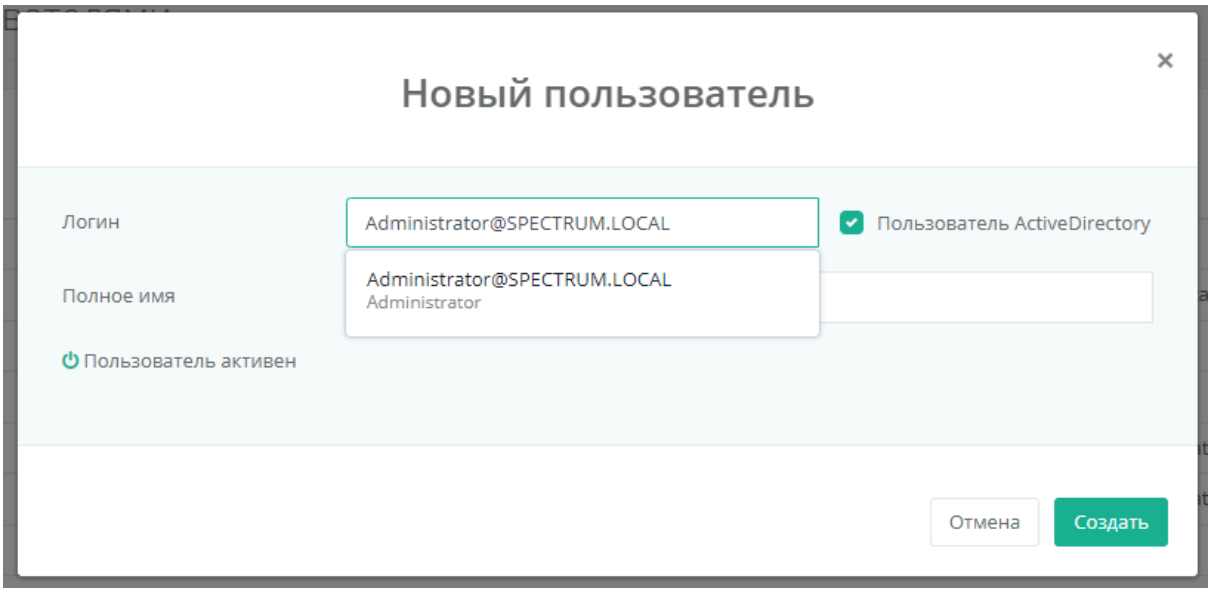


Рис.: Создание доменного пользователя

Пользователя можно отредактировать, нажав на иконку карандаша напротив соответствующего пользователя, в появившемся диалоговом окне изменить данные пользователя и нажать кнопку “Сохранить”, см. пример ниже:

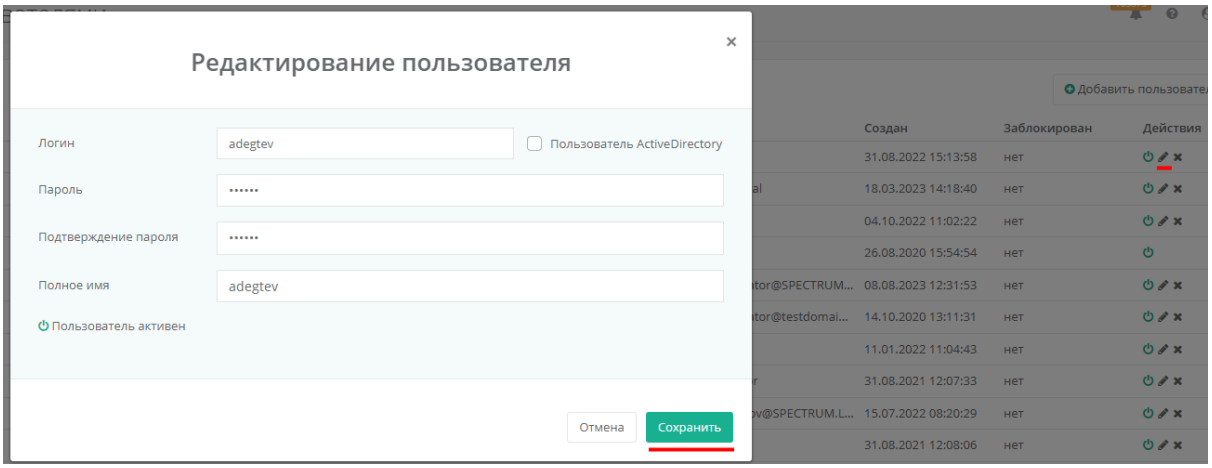


Рис.: Редактирование пользователя

Пользователя можно заблокировать или разблокировать, нажатием на зеленую/красную иконку со знаком включить напротив соответствующего пользователя.

Пользователя можно удалить из системы “Спектр”, нажатием на иконку “x” напротив соответствующего пользователя, и подтвердить удаление нажав кнопку “Удалить”, см. пример ниже:

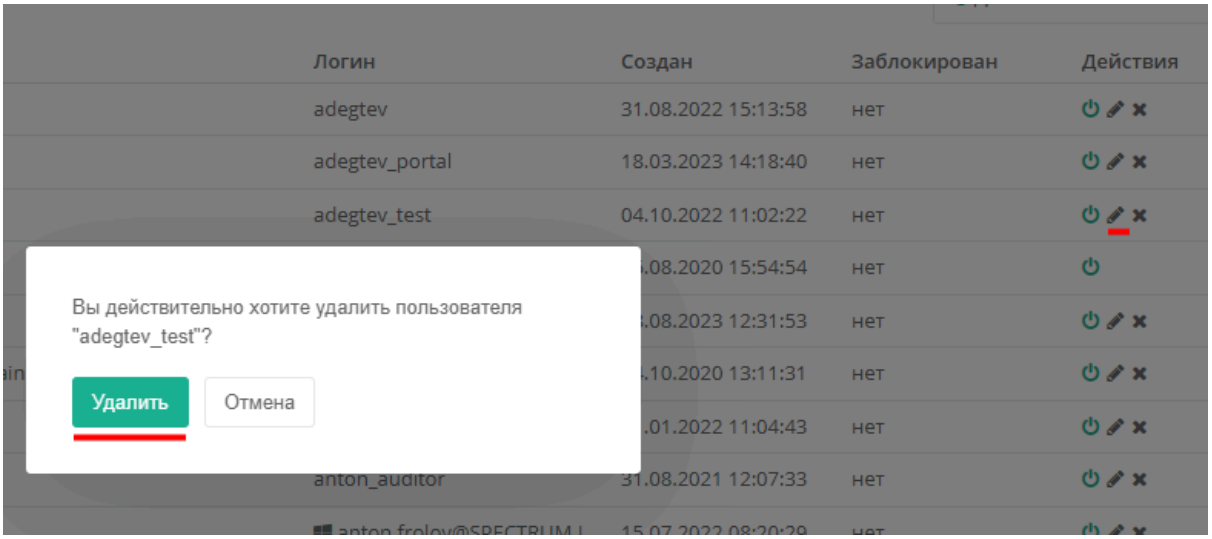


Рис.: Удаление пользователя

Встроенного пользователя “admin” нельзя удалить, заблокировать и отредактировать.

4.3.10. Просмотр журнала действий пользователей системы

Все действия пользователей с элементами управления системы “Спектр. Маркер” регистрируются в специальных журналах. Просмотр журнала действий пользователей доступен в разделе “Журналы -> Действия пользователей”.

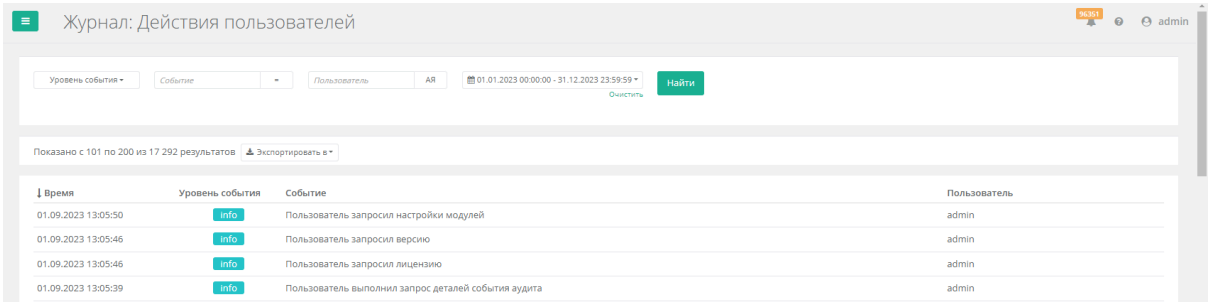


Рис.: Журнал действий пользователей

Журнал представлен в виде таблицы. Для каждого сообщения в журнале присутствует следующая информация:

- Время - дата и время регистрации события;
- Уровень логирования - уровень важности сообщения. В системе присутствуют следующие уровни логирования:
    - Info
    - Warning
    - Error
    - Critical
- Событие - детализированное описания события;
- Пользователь - учетная запись пользователя системы “Спектр”, выполнившего действие.

В таблице возможны следующие действия над отображаемыми данными:

- Сортировка записей по всем столбцам - осуществляется щелчком мыши по заголовку столбца;
- Фильтрация данных по содержимому каждого поля журнала. Фильтрация доступна в верхней части экрана.

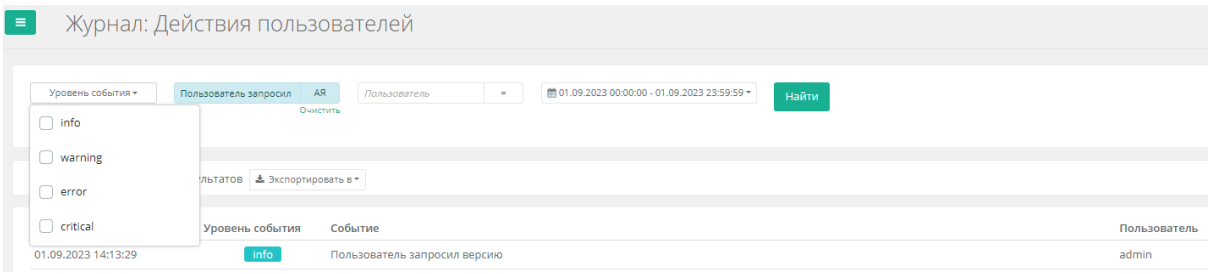


Рис.: Фильтрация журнала действий пользователей

Для того, чтобы отфильтровать нужные записи журнала необходимо заполнить поля ввода соответствующих фильтров и нажать кнопку “Найти”.

4.3.11. Просмотр журнала системных событий

Различные события, связанные с функционирование модулей системы “Спектр. Маркер” (системные события) регистрируются в специальном журнале. Просмотр журнала системных событий доступен в разделе “Журналы” -> “Системные события”.

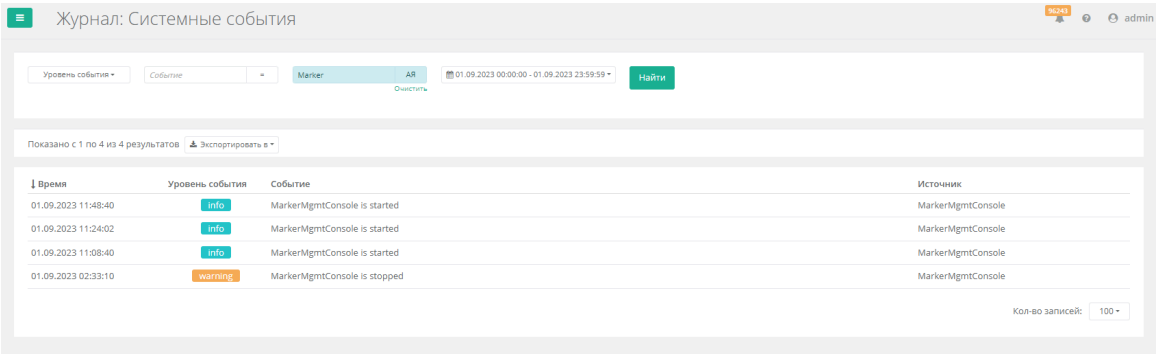


Рис.: Журнал системных сообщений

Журнал представлен в виде таблицы. Для каждого сообщения в журнале присутствует следующая информация:

- Время - дата и время регистрации события;
- Уровень логирования - уровень важности сообщения. В системе присутствуют следующие уровни логирования:
    - Info
    - Warning
    - Error
    - Critical
- Событие - детализированное описания события;
- Источник - модуль системы “Спектр”, инициировавший событие.

В таблице возможны следующие действия над отображаемыми данными:

- Сортировка записей по всем столбцам - осуществляется щелчком мыши по заголовку столбца;
- Фильтрация данных по содержимому каждого поля журнала. Фильтрация доступна в верхней части экрана.

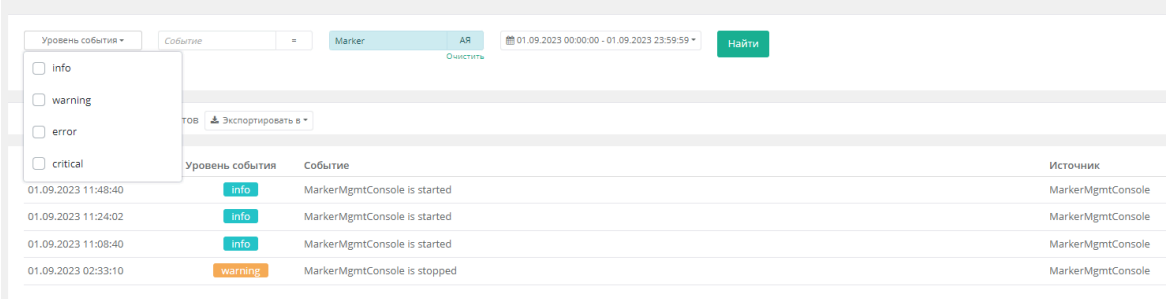


Рис.: Фильтрация журнала системных сообщений

Для того, чтобы отфильтровать нужны записи журнала необходимо заполнить поля ввода соответствующих фильтров и нажать кнопку “Найти”.

4.3.12. Просмотр информации о системе

Посмотреть версию системы можно нажав на иконку “?” в верхнем меню, и нажать на пункт “О продукте”, см. на рисунке ниже

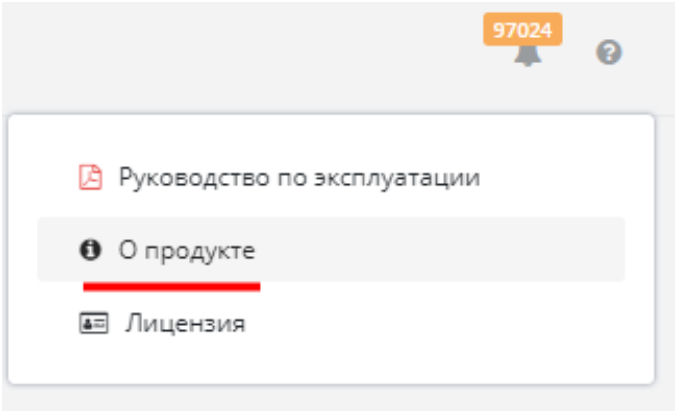


Рис.: Кнопка перехода в раздел “О продукте”

Откроется раздел с информацией о системе с версиями компонентов, см. пример ниже:

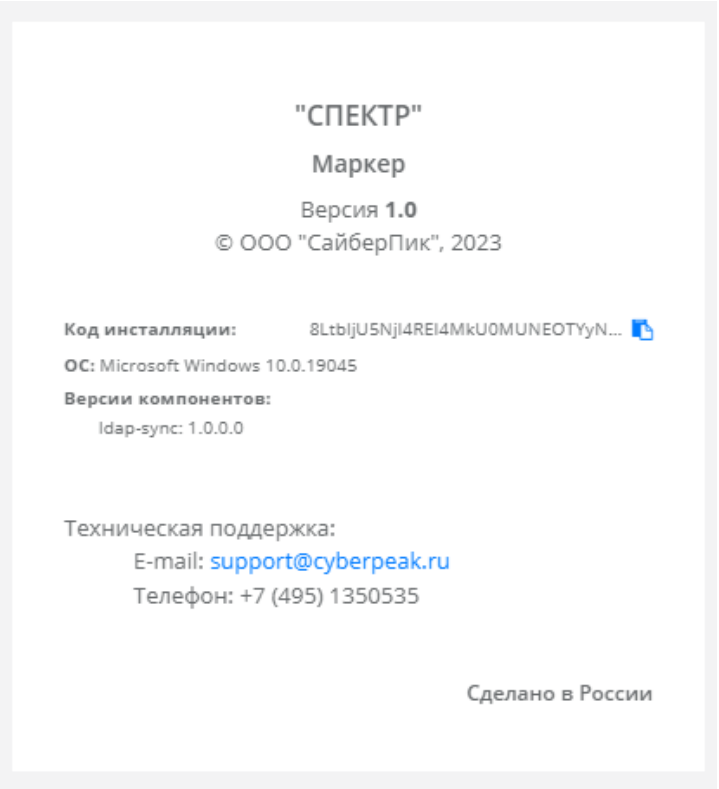


Рис.: О продукте. Версии компонентов

Также в данном разделе можно скопировать “код инсталляции” и отправить его техподдержке, для получения файла лицензии. Для загрузки лицензии необходимо нажать на иконку “?” в верхнем меню, и нажать на пункт “Лицензия”, см. рис. ниже

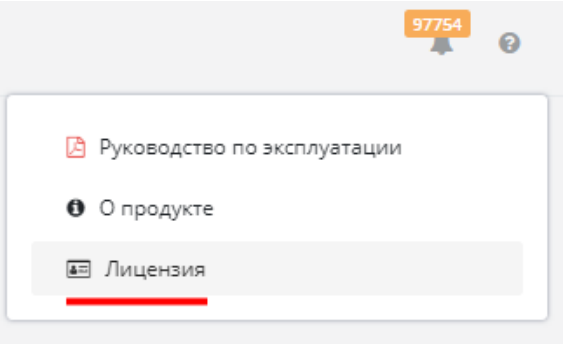


Рис.: Кнопка перехода в раздел “Лицензия”

В появившемся окне нажать на кнопку “Загрузить лицензию” и выбрать полученный файл лицензии.

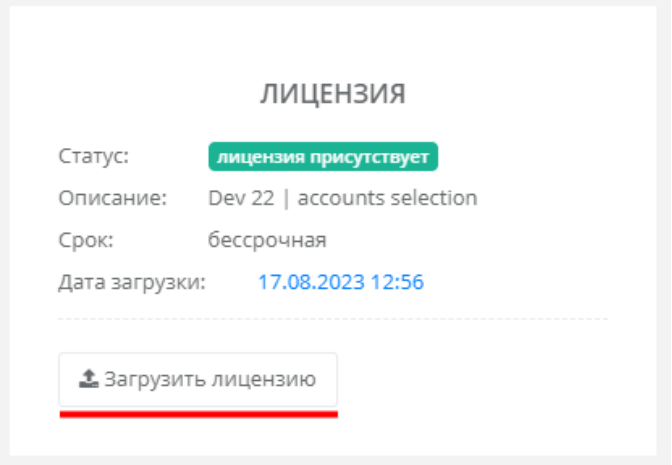


Рис.: Загрузка лицензии

Скачать данное руководство по эксплуатации нажав на иконку “?” в верхнем меню, и нажать на пункт “Руководство по эксплуатации”, см. на рисунке ниже:

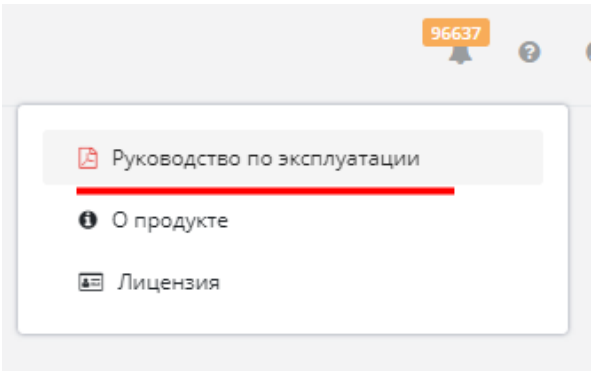


Рис.: Скачать руководство по эксплуатации

4.3.13. Диагностическая информация

В раздел “Диагностической информации” можно перейти из главного меню раздел “Диагностика”. В нем отражаются состояния различных сервисов. А так же можно выполнить сбор диагностической информации нажатием на соответствующую кнопку, см. рис. ниже:

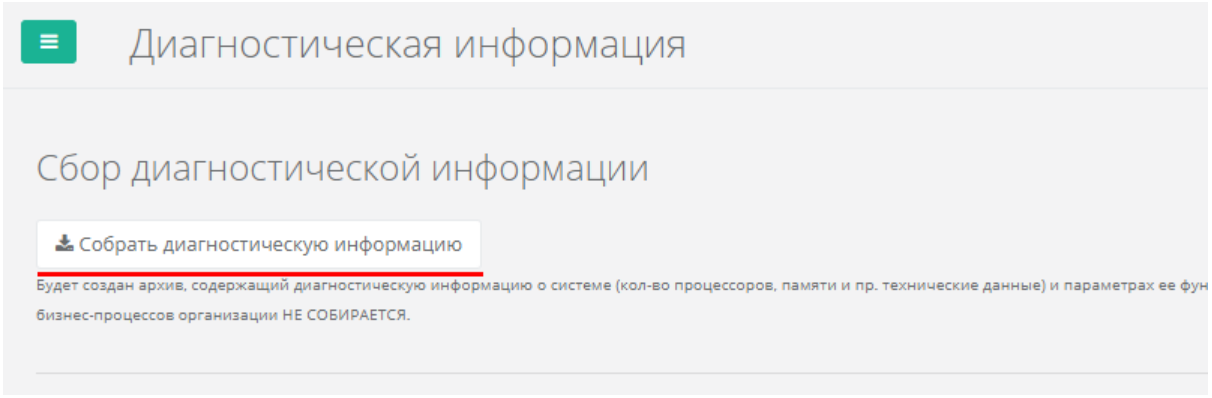


Рис.: Сбор диагностической информации

5. Работа с клиентским приложением классификации данных

5.1. Установка агентского ПО “Маркер”

Агентское ПО “Маркер” может быть установлено на следующие операционные системы:

- MS Windows Server 2008 R2;
- MS Windows Server 2012 и новее;
- MS Windows 7 и новее

Требования к ресурсам и нагрузка, создаваемая\потребляемая агентом:

- Тип нагрузки: постоянная:
- CPU: <2% (при мощности ядра ~2.2 ГГц);
- RAM: 50 - 80 Mb;
- HDD: до 100 Mb (зависит от размера локального хранилища, настраивается из UI)

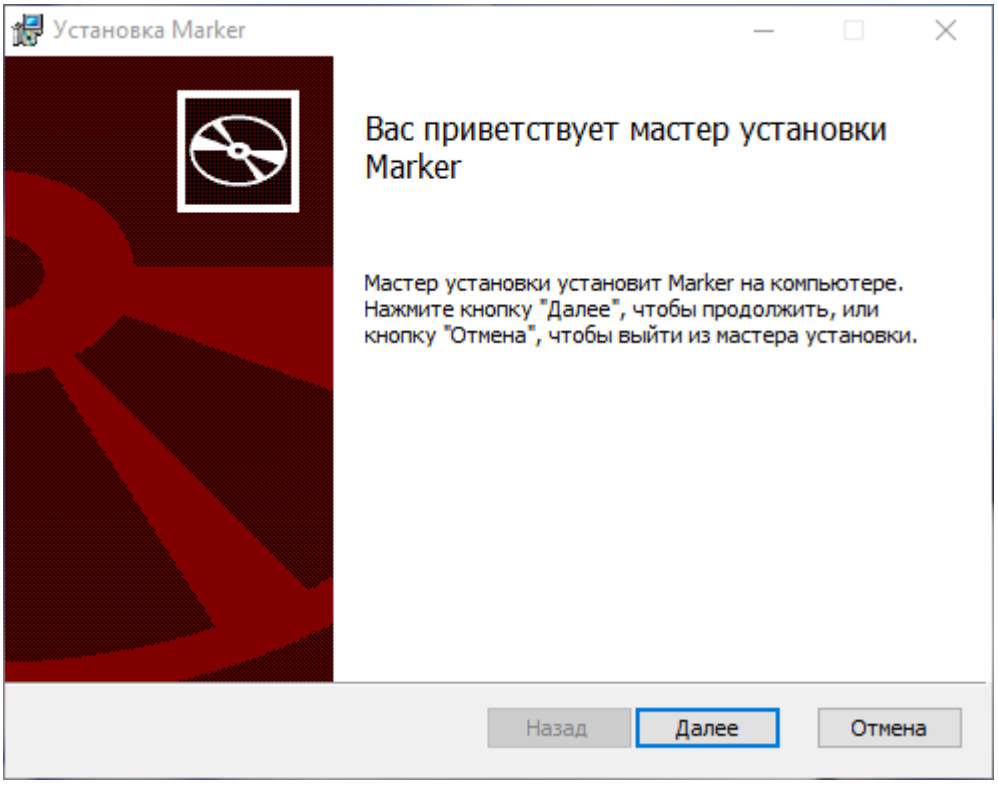
5.1.1. Установка агентского ПО “ Маркер” на файловые хранилища под управлением ОС семейства MS Windows

Перед установкой агентского ПО на рабочее место с операционной системой семейства MS Windows необходимо установить .NET Framework версии 4.7.2 или выше (если не установлен). Для этого скопируйте на хранилище и запустите файл *ndp472-kb4054530-x86-x64-allos-enu.exe*, далее следуйте инструкциями программы-установщика.
Данный файл можно скачать по ссылке: https://dotnet.microsoft.com/en-us/download/dotnet-framework/net472

Важно: установка/обновление версии .NET Framework может запросить перезагрузки операционной системы.

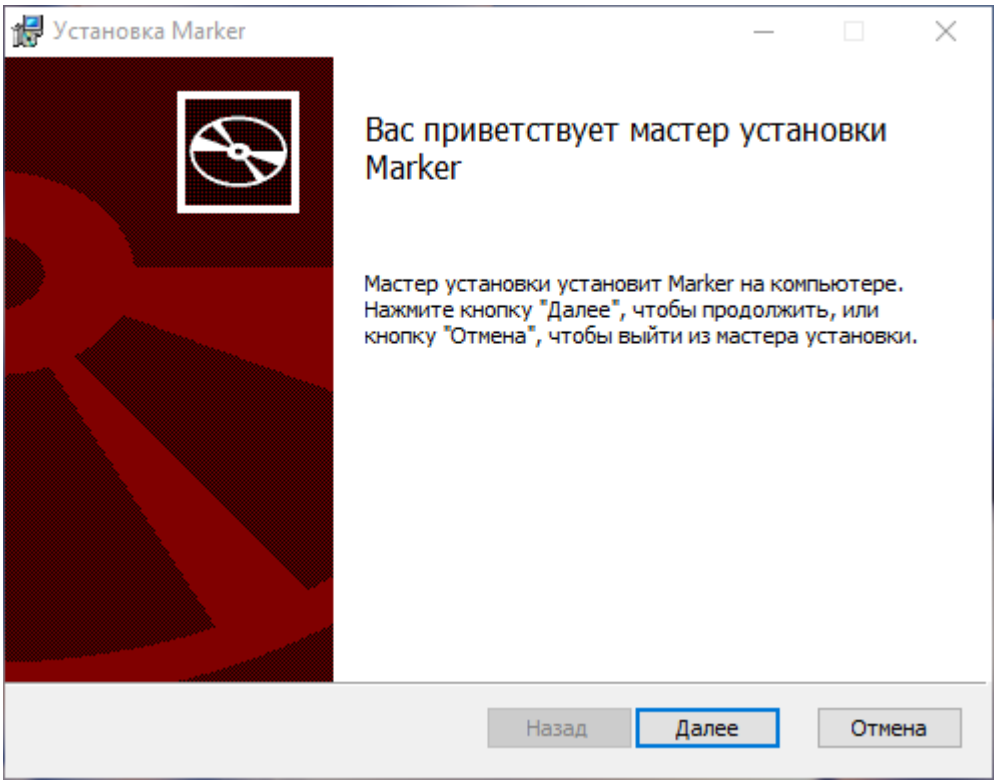
Для установки надстроек Ms Office на ОС MS Windows 11 может также понадобиться VS Tools for Office Runtime. Для установки скопируйте на рабочую станцию и запустите файл *vstor_redist.exe* *https://www.microsoft.com/en-us/download/details.aspx?id=48217*, далее следуйте инструкциями программы-установщика.

Для установки агентского ПО “Маркер” необходимо скопировать установочный пакет *Marker_x.x.msi* на файловый сервер и запустить его (например, дважды кликнув на msi-файл) от имени администратора. После чего откроется окно инсталлятора агента “Маркер”. В нем необходимо нажать кнопку “Далее”:



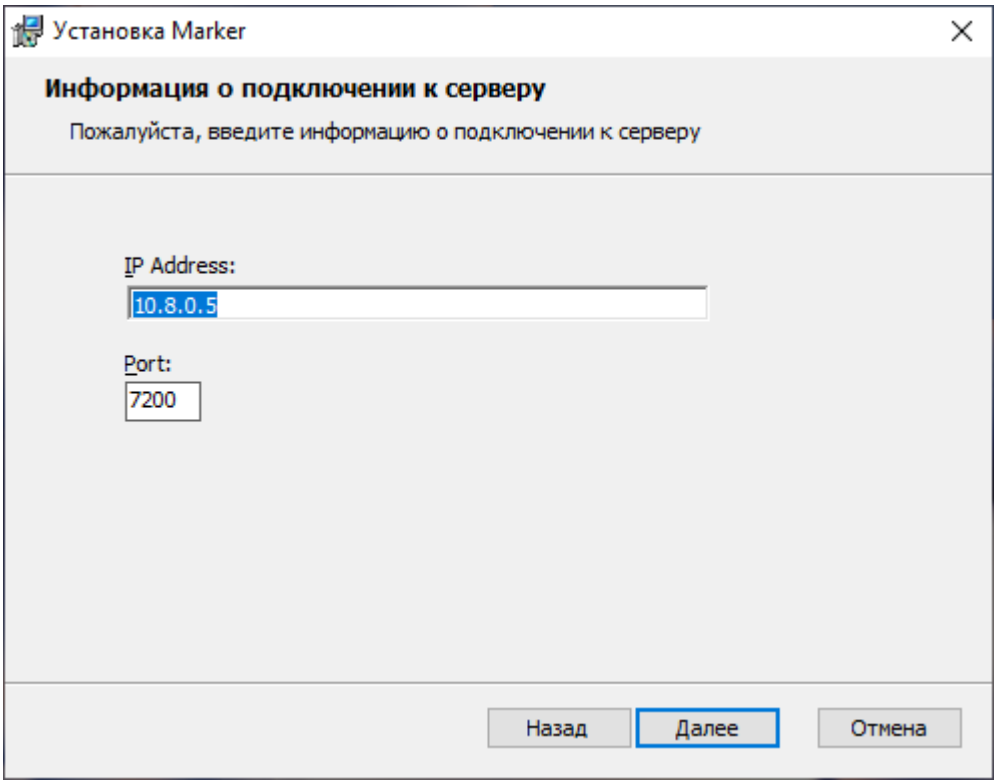
*Окно установки агента "*Маркер*"*

На следующем шаге необходимо принять лицензионное соглашение и также нажать "Далее".



*Окно установки агента "*Маркер*": принятие лицензионного соглашения*

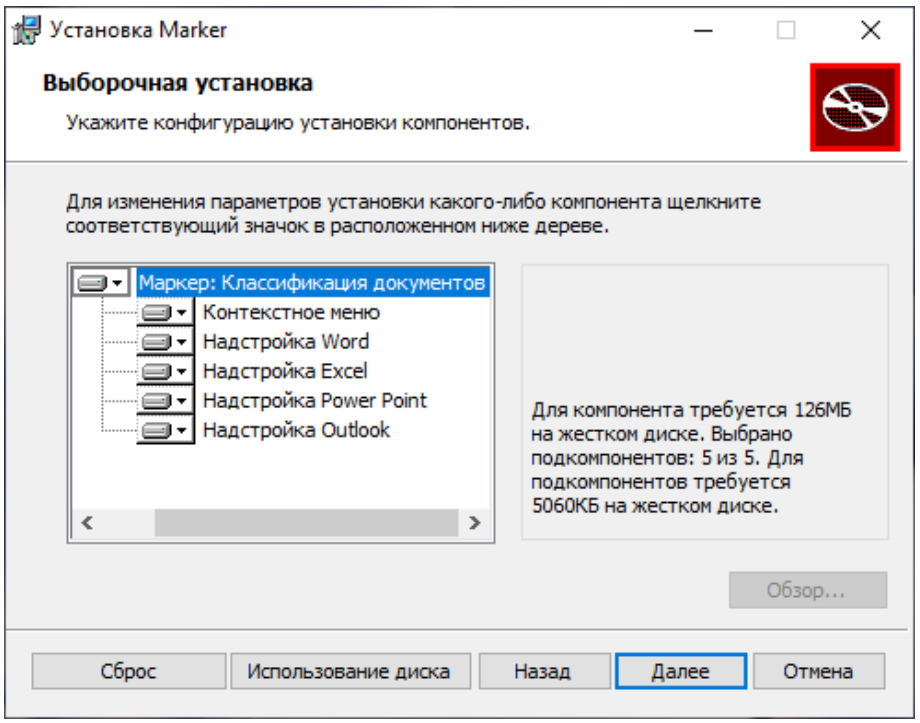
На следующем шаге важно корректно заполнить IP-адрес сервера “Маркер” и порт, на который будет подключаться агентское ПО (по умолчанию, 7200):



Окно установки агента “Маркер”: указание IP-адреса сервера “Маркер” и порт

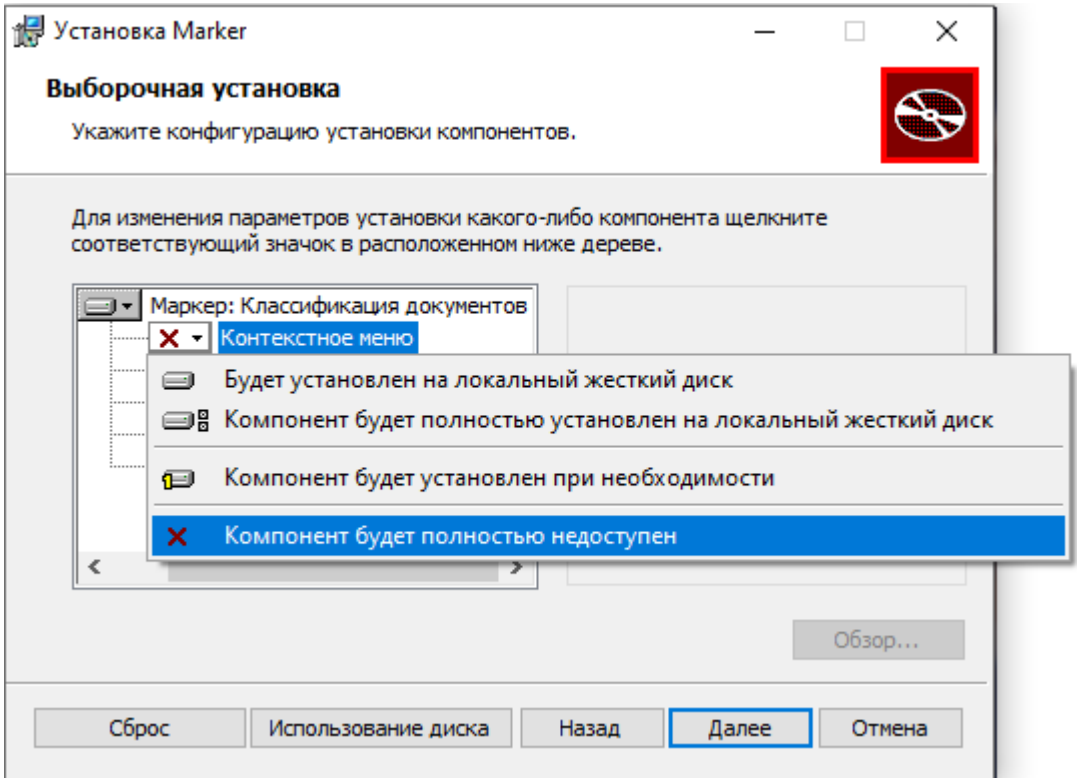
Далее необходимо выбрать, какое ПО следует установить:

- Контекстное меню;
- Надстройка Ms Word;
- Надстройка Ms Excel;
- Надстройка Ms Power Point;
- Надстройка Ms Outlook;



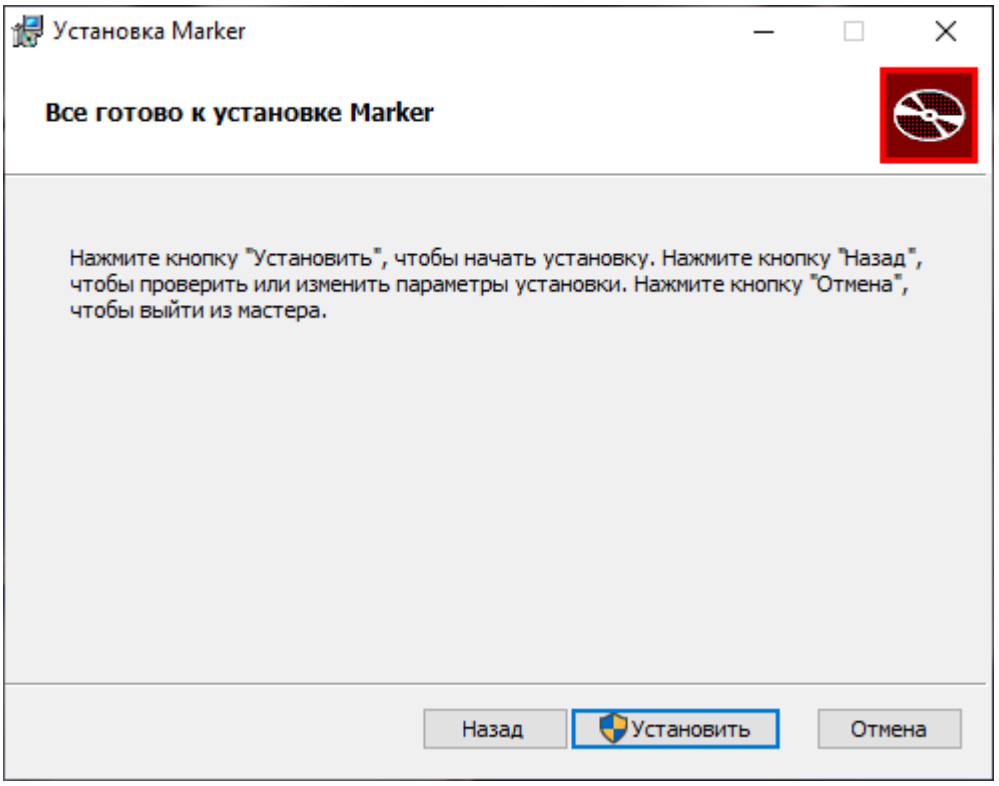
Окно установки агента “Маркер”: выбор компонентов

По умолчанию, будут установлены все доступные компоненты. Для отключения соответствующих компонент необходимо установить “крестик”: “Компонент будет полностью недоступен”.



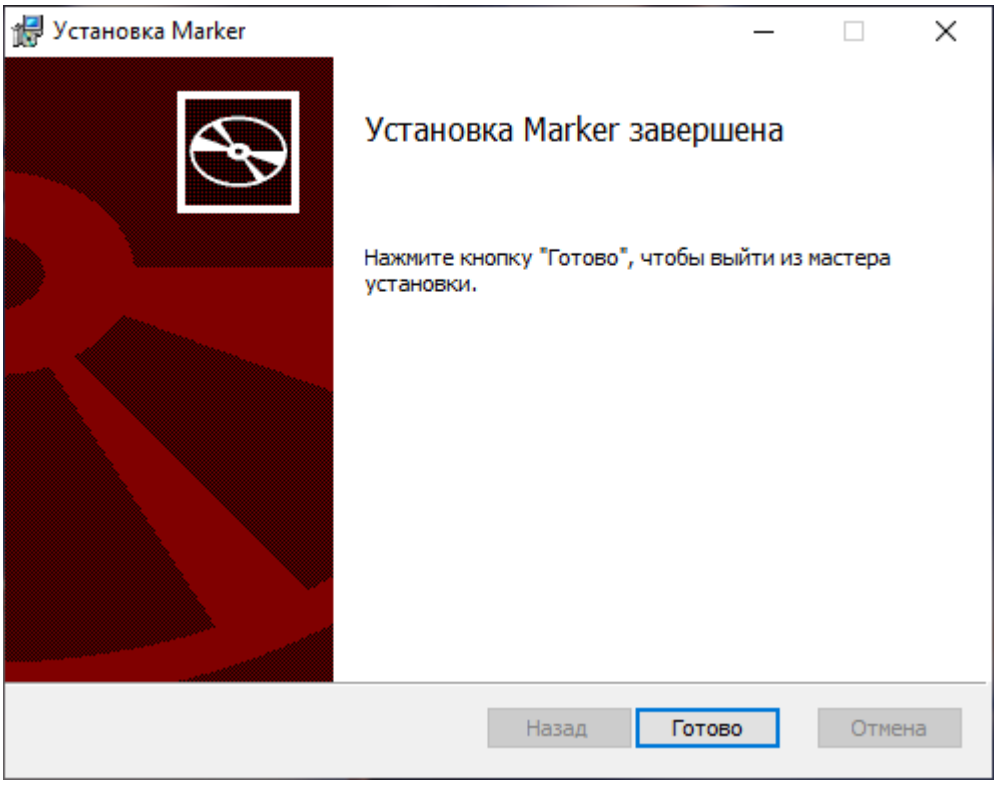
Окно установки агента “Маркер”: выбор компонентов

Далее необходимо нажать “Далее” и на следующем шаге “Установить”.



Окно установки агента “Маркер”: установка

После завершении процесса установки необходимо нажать кнопку “Готово”:



Окно установки агента “Маркер”: завершение установки

Для установки агента в фоновом режиме без использования интерфейса программы-инсталлятора необходимо запустить приложение “Командная строка” от имени администратора и выполнить следующую команду:

```
msiexec /i Marker_x.x.msi REMOTE_HOST=X.X.X.X REMOTE_PORT=7200 /qn
/norestart
```

где:

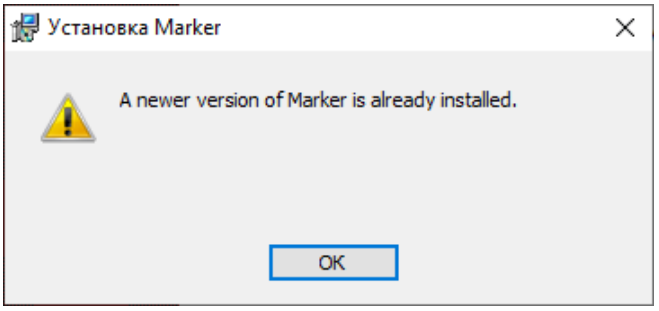
- Marker_x.x.msi - путь до установочного пакета;
- X.X.X.X - доменное имя или IP-адрес сервера “Маркер”.

Данную команду также можно использовать для установки агента удаленно, используя стандартные средства администрирования.

5.1.2. Обновление агентского ПО “Маркер” на файловых хранилищах под управлением ОС семейства MS Windows

Для обновления агентского ПО “Маркер” необходимо скопировать установочный пакет *Marker_x.x.msi* более новой версии на файловый сервер и запустить его (например, дважды кликнув на msi-файл) от имени администратора. После чего произвести установку новой версии, согласно п. 4.1.1 “Установка агентского ПО “Маркер””.

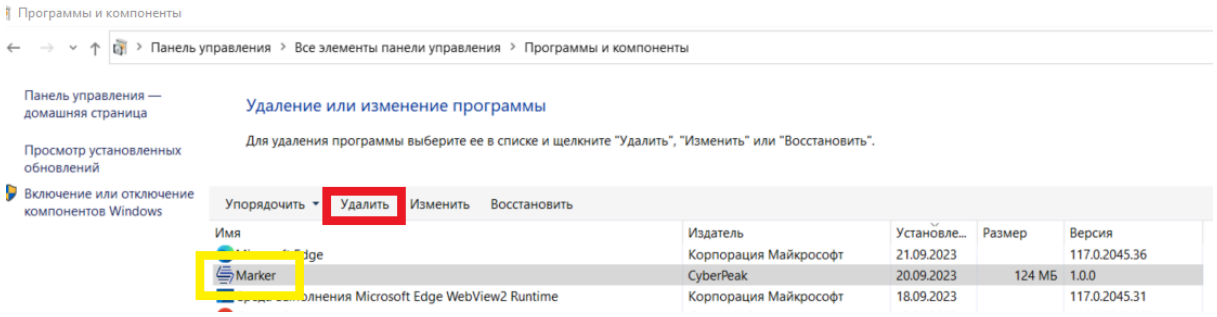
В случае, если на файловом хранилище уже установлена более новая версия ПО “Маркер”, будет показано предупреждение и установка будет отменена.



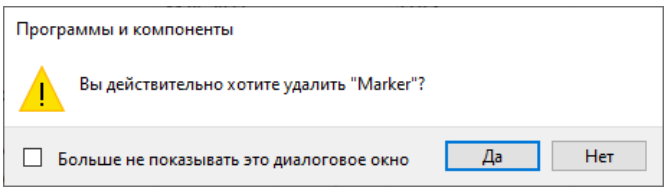
Для установки более старой версии продукта необходимо сначала выполнить удаление согласно п. 4.1.3 “Удаление агентского ПО “Маркер””, а затем уже произвести установку согласно п. 4.1.1 “Установка агентского ПО “Маркер””.

5.1.3. Удаление агентского ПО “ Маркер” с файловых хранилищ под управлением ОС семейства MS Windows

Для удаления агентского ПО “Маркер” необходимо запустить установочный пакет *Marker_x.x.msi.* Для этого необходимо выбрать *“Панель управления” -> “Программы и компоненты” -> “Marker”:*



Выбрать “Удалить” или дважды кликнуть мышкой по компоненту. Подтвердить удаление компонента “Marker”:



Далее дождаться завершения удаления ПО. Для удаления компонента “Marker” потребуются права администратора.

5.2. Классификация документов с помощью агентского ПО “Маркер”

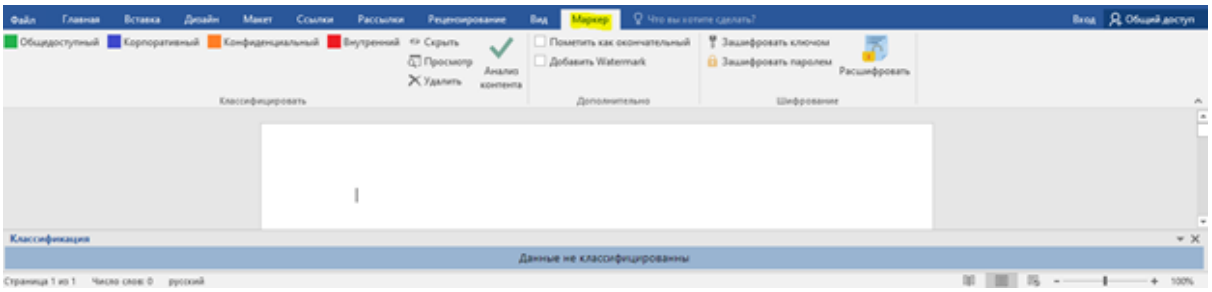
Для офисных документов формата *.docx, .xlsx, .pptx* метка проставляется во внутренние свойства документа, а также дублируется в Альтернативные потоки данных. Для всех остальных типов документов метка будет проставлена только в Альтернативные потоки данных.

Метки для классификации документа, а также соответствующие им политики и настройки, будут отображены после получения информации с сервера “Маркер”. Для обновления надстройки после получения/изменения информации с сервера потребуется перезагрузка приложения MS Office.

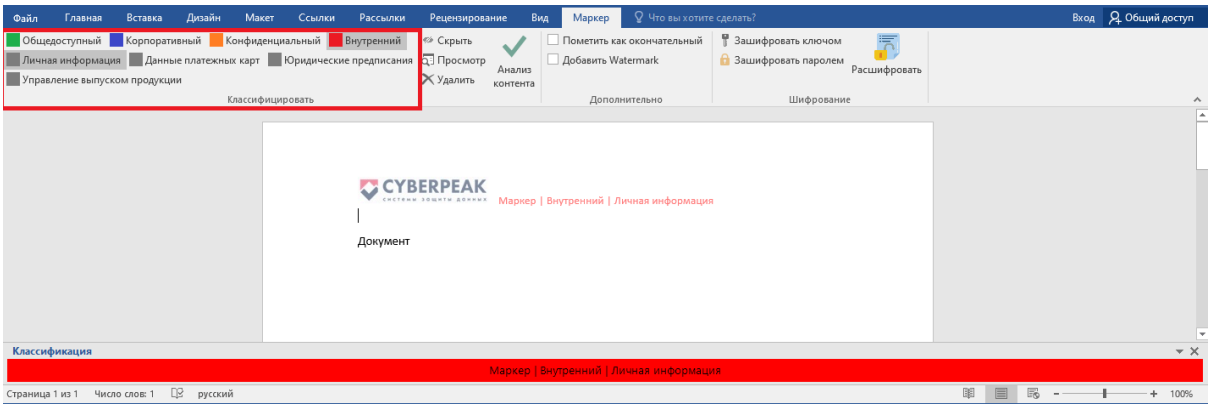
5.2.1. Классификация документов с помощью надстройки MS Office

После установки соответствующей надстройки в приложении появится новая вкладка “Маркер”, а также снизу отобразится панель с информацией о текущей классификации

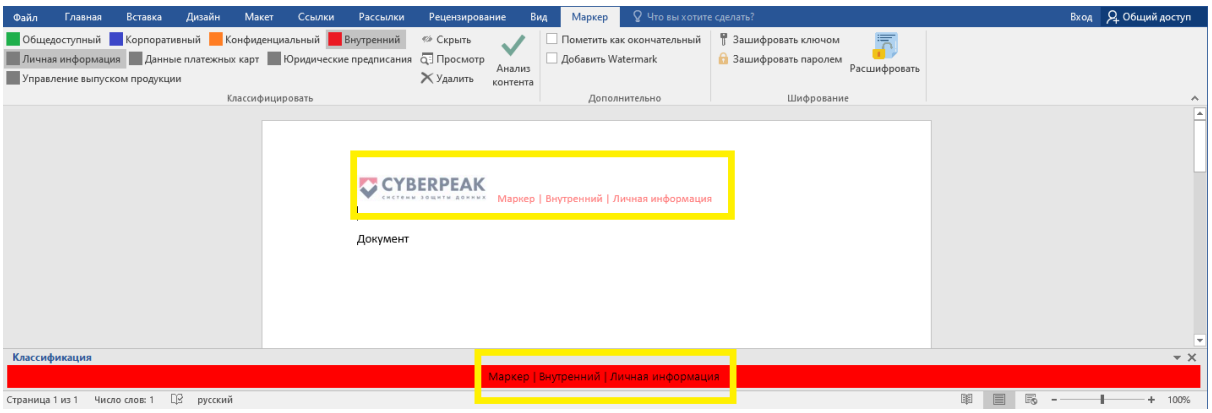
документа:


Файл
Главная
Вставка
Дизайн
Макет
Ссылки
Рассылки
Рецензирование
Вид
Маркер
Что вы хотите сделать?
Вход
Общий доступ
Общедоступный
Корпоративный
Конфиденциальный
Внутренний
Скрыть
Просмотр
Удалить
Анализ контента
Классифицировать
Пометить как окончательный
Добавить Watermark
Дополнительно
Зашифровать ключом
Зашифровать паролем
Расшифровать
Шифрование
Классификация
Данные не классифицированы
Страница 1 из 1
Число слов: 0
русский
100%

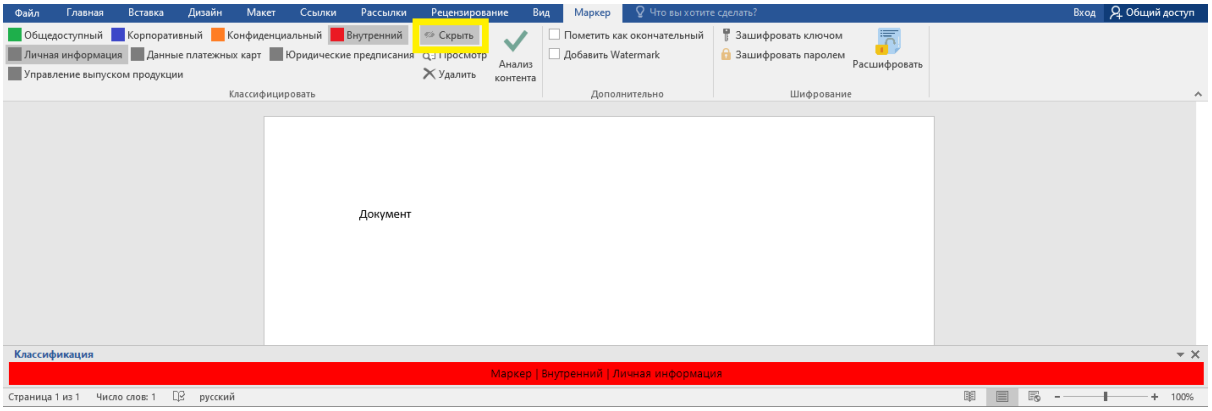
Для классификации документа выберете одну из меток первого уровня, и при необходимости проставьте метки второго уровня.



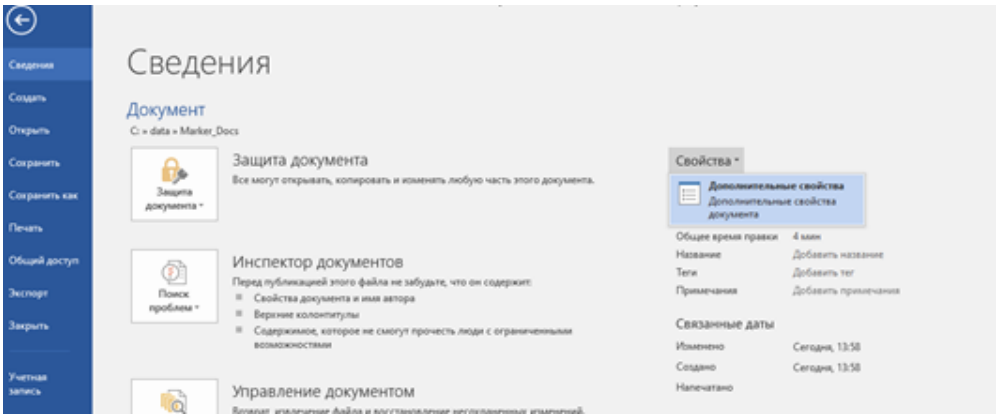
Обновленная классификация документа отобразится в колонтитуле, а также на панели информации снизу. Для сохранения классификации в документе необходимо сохранить файл.



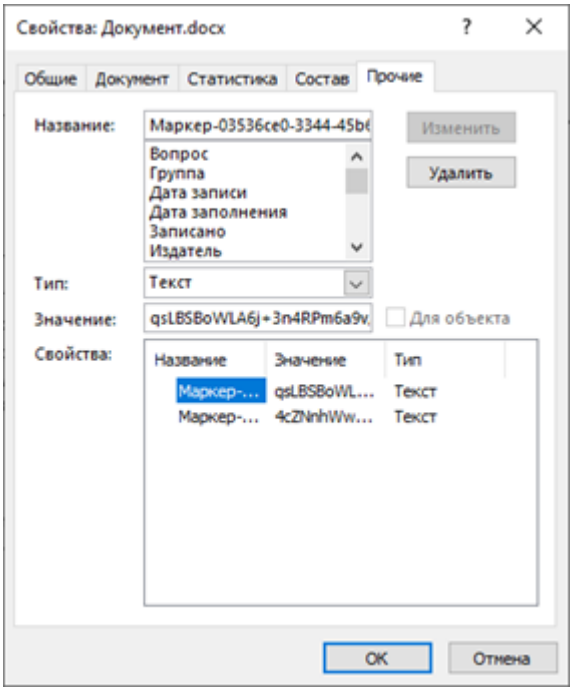
Скрыть отображение классификации документа в колонтитуле можно нажав кнопку “Скрыть”. Вернуть отображение классификации документа в колонтитуле можно повторно нажав кнопку “Скрыть”.



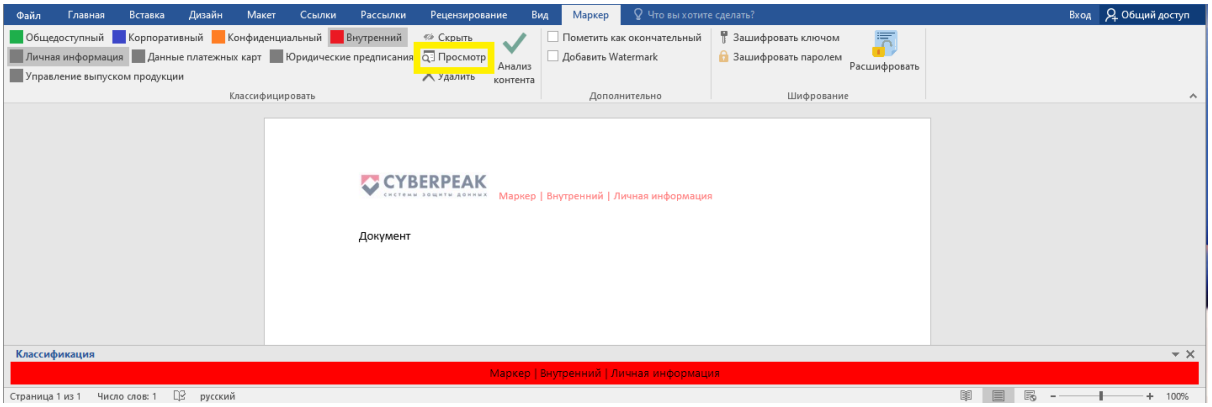
Просмотреть проставленную метку можно в свойствах документа, выбрав *Файл -> Сведения -> Свойства -> Дополнительные свойства:*



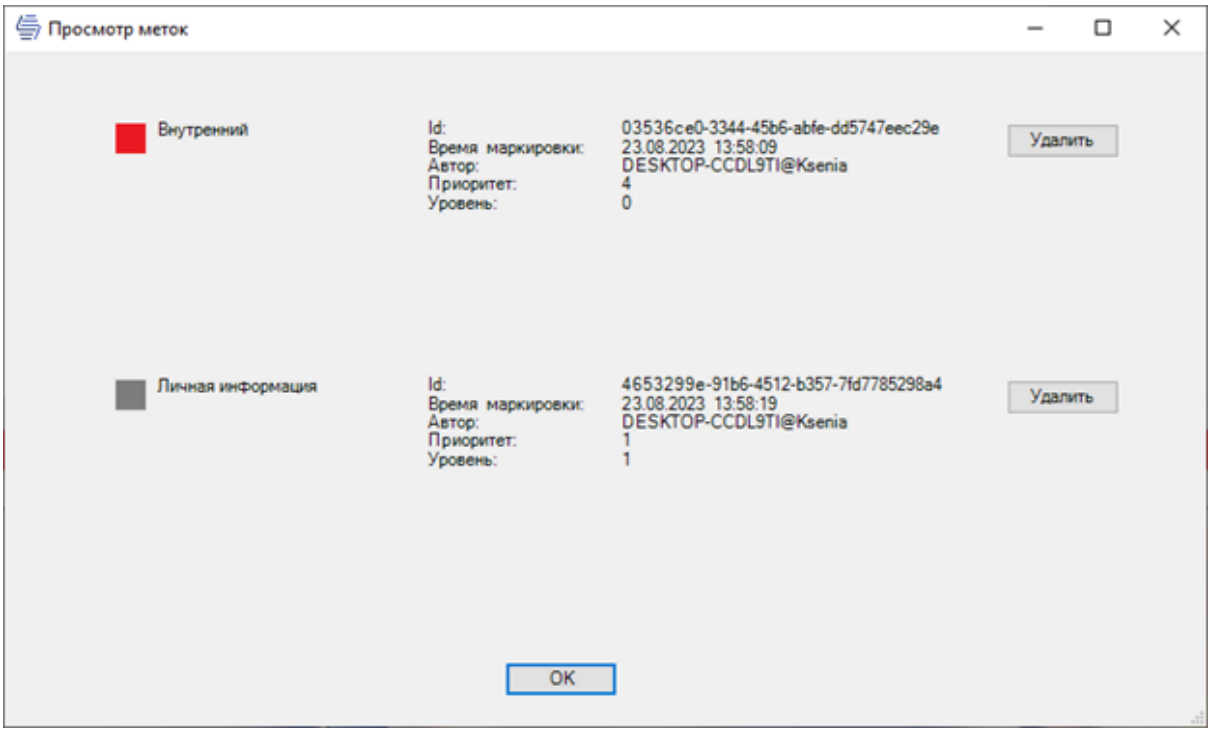
В диалоговом окне свойств выбрать вкладку “Прочие”. Можно убедиться в наличии дополнительных свойств документа с префиксом “Маркер”:



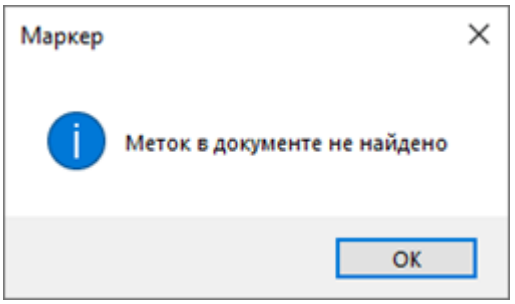
Для просмотра всех существующих меток в документе необходимо нажать кнопку “Просмотр”:



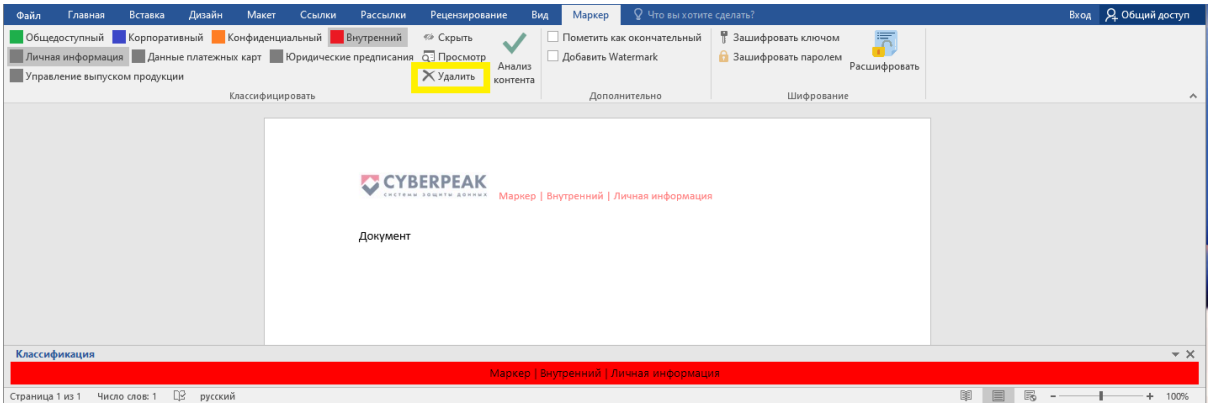
При наличии меток в документе отобразится диалоговое окно, с основной информацией по существующим меткам. При необходимости можно удалить любую метку. При удалении метки первого уровня все метки будут удалены из документа



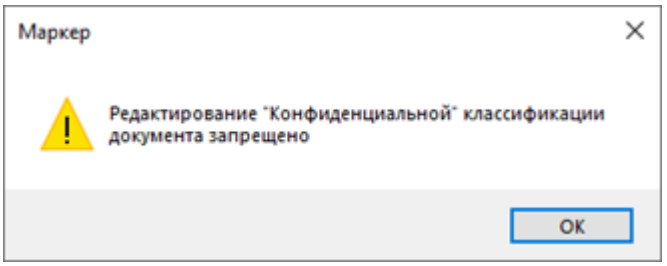
В случае отсутствия меток в документе выводится информационное сообщение



Для очищения классификации документа можно удалить все метки нажав кнопку “Удалить”:

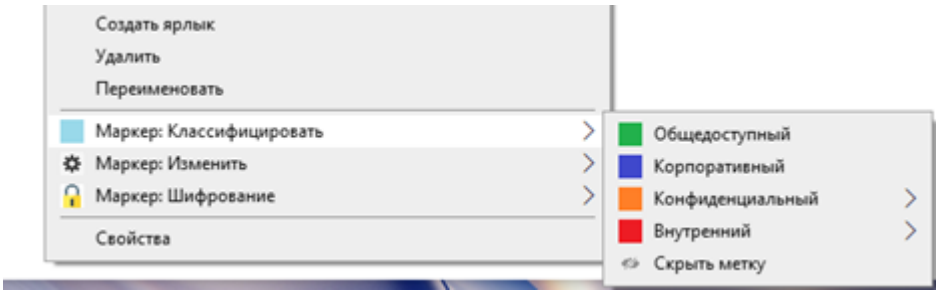


При изменении классификации документа срабатывает “Политика ограничений действий с метками”. При запрете изменения соответствующей классификации документа появится всплывающее сообщение:



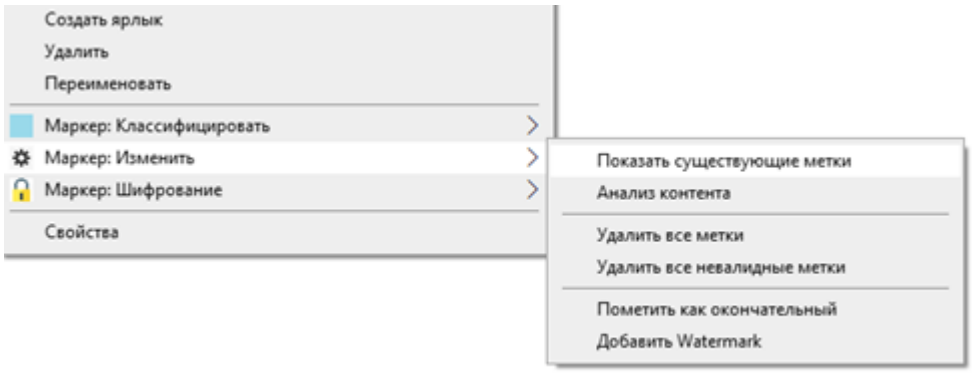
5.2.2. Классификация документов с помощью контекстного меню

После установки агента в контекстном меню всех документов появится новый раздел “Маркер”:



Для обновления классификации выберите пункт меню *Маркер: Классифицировать -> Выберите соответствующую классификацию для документа*.

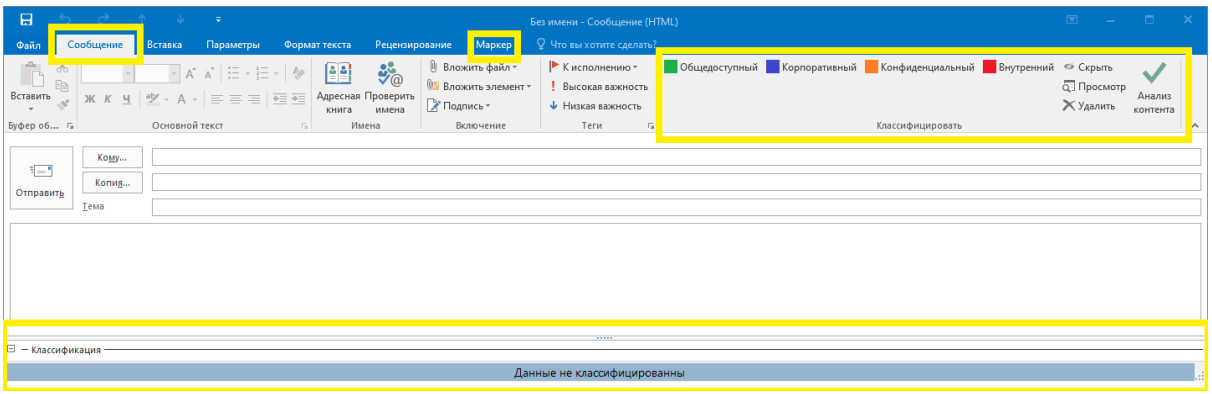
Для просмотра или изменения текущей классификации документа выберите пункт меню *Маркер: Изменить -> Выберите действие*



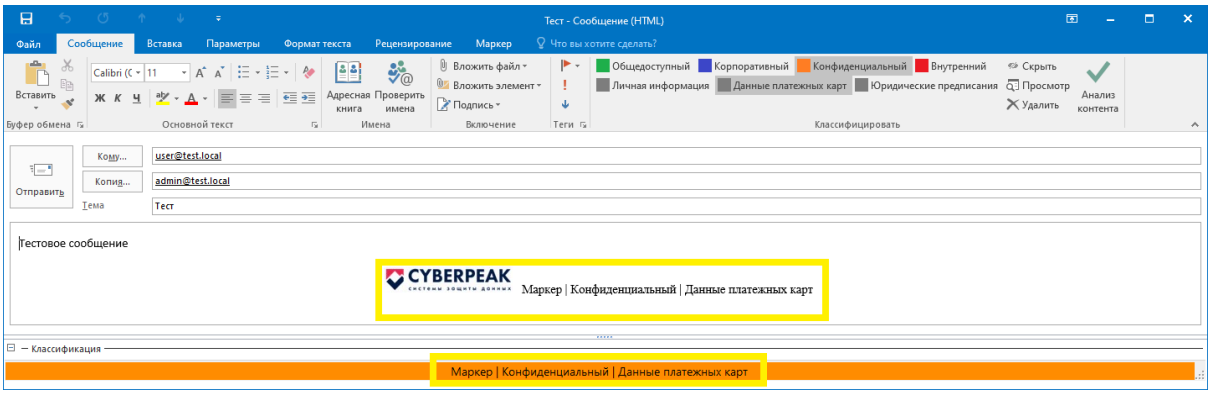
При изменении классификации документа так же срабатывает “Политика ограничений действий с метками”.

5.2.3. Классификация писем с помощью надстройки MS Outlook

После установки соответствующей надстройки в приложении при работе с сообщениями появится новая вкладка “Маркер”, а также снизу отобразится панель с информацией о текущей классификации документа. На вкладках “Сообщение” и “Маркер” появится новый раздел настроек для классификации:



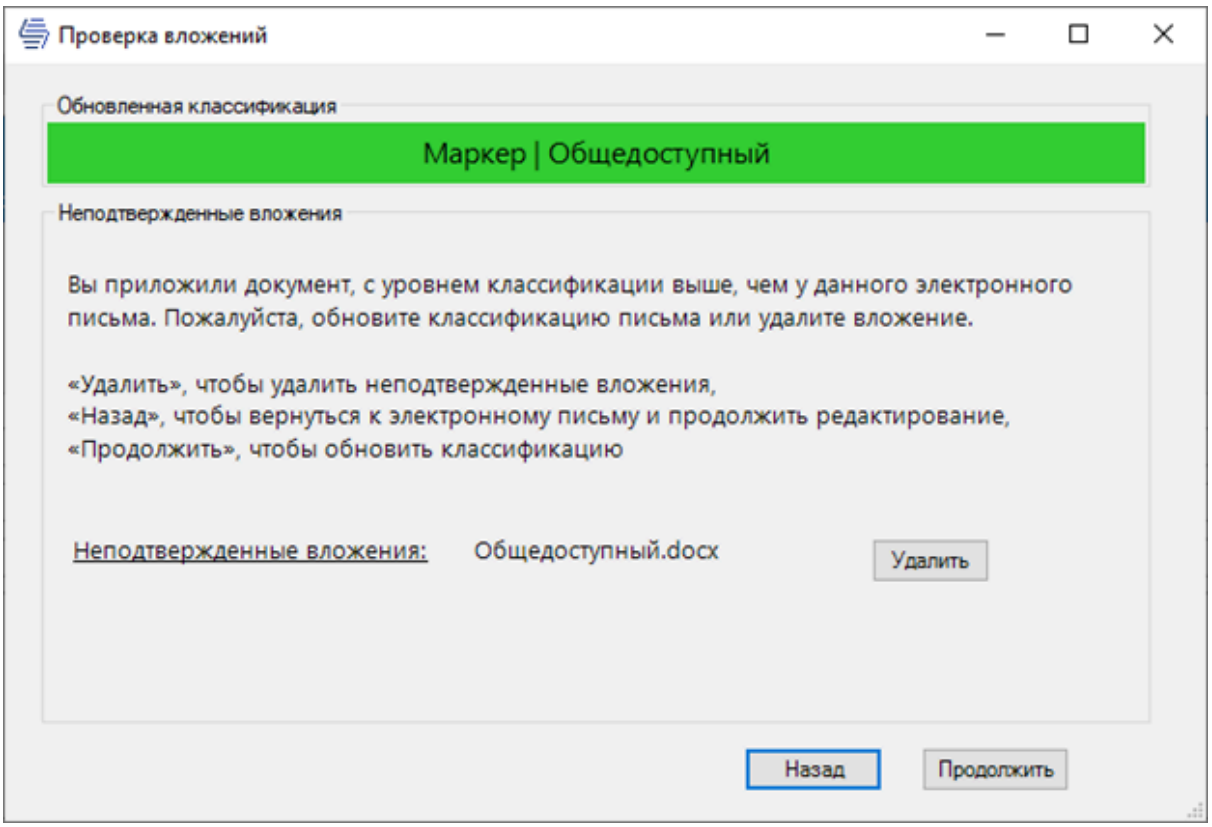
Для классификации документа можно выбрать одну из меток первого уровня, и при необходимости проставить метки второго уровня. Обновленная классификация документа отобразится в сообщении, а также на панели информации снизу:



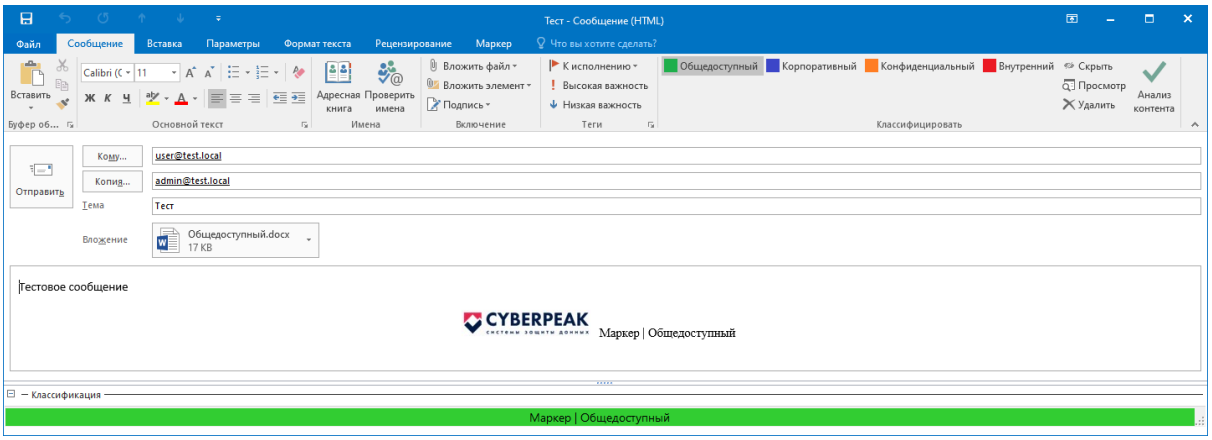
Классификацию для сообщения можно также скрыть/показать из тела письма нажав кнопку “Скрыть”. Также можно просмотреть/удалить существующие метки нажав кнопки “Просмотр”, “Удалить”.

При добавлении вложений в сообщение срабатывают политики, заданные на сервере “Маркер”.

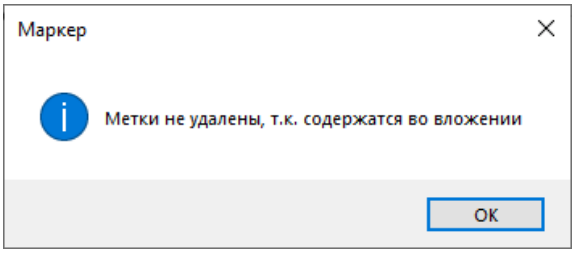
При вложении документа с меткой срабатывает “Политика классифицированных вложений” и всплывает информационное окно при необходимости повышения уровня классификации письма:



Для подтверждения добавления вложения к письму необходимо нажать кнопку “Продолжить”, при этом классификация письма обновится:

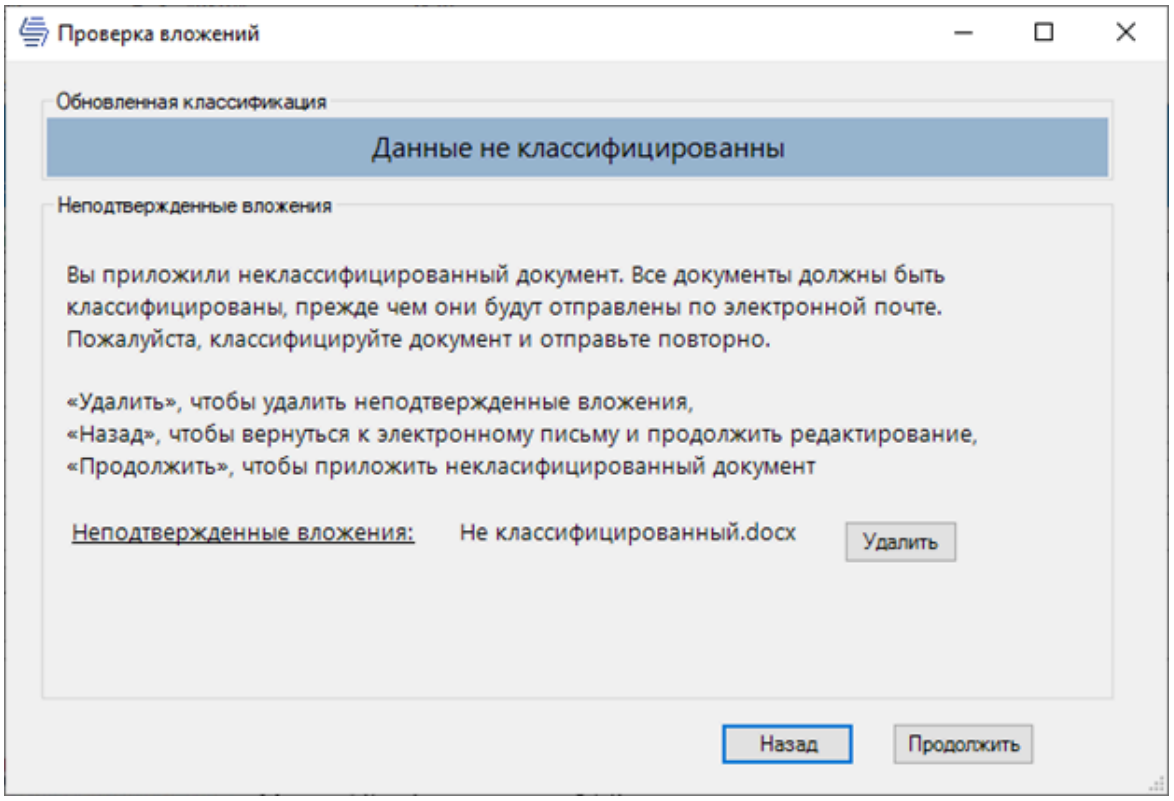


Уровень классификации письма может быть выше уровня классификации вложения. Однако, удалить классификацию письма при наличии классифицированного вложения нельзя.

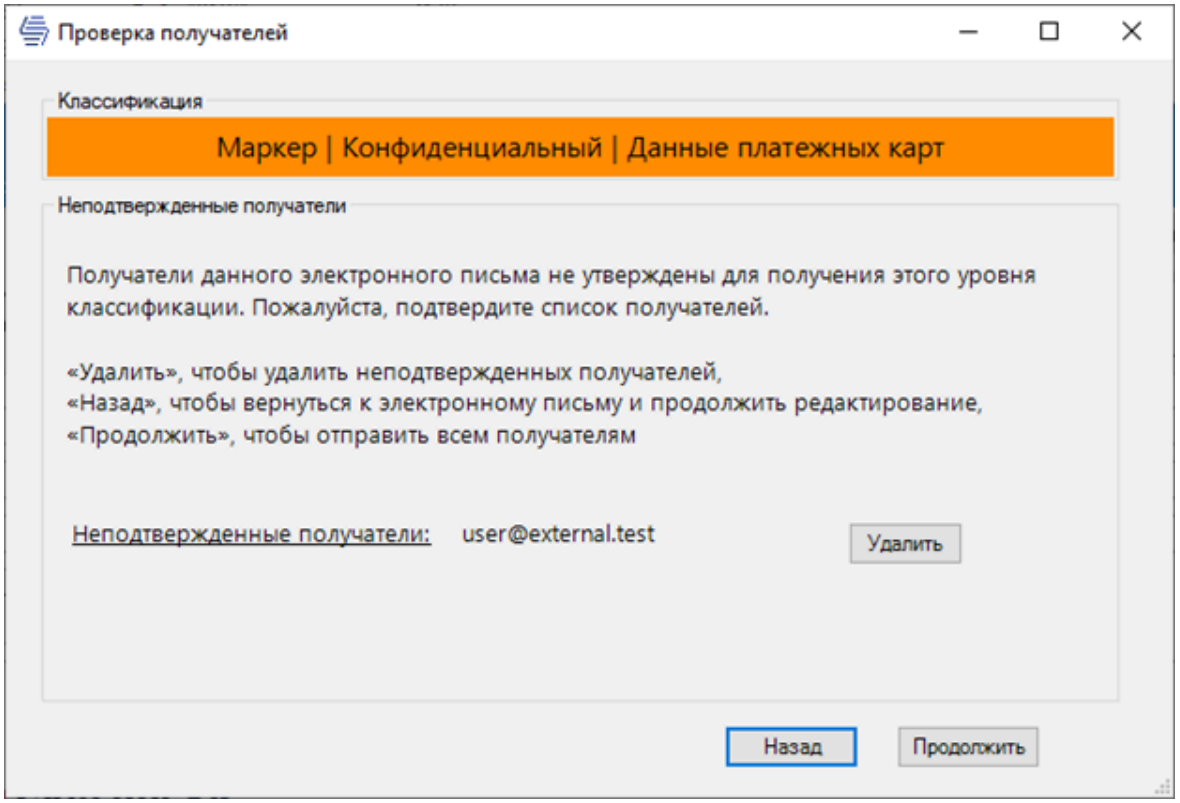


Для понижения уровня классификации письма потребуется удалить вложение.

При вложении неклассифицированного офисного документа срабатывает “Политика неклассифицированных вложений” и всплывает информационное окно:



При отправке сообщения срабатывает “Политика отправки электронных писем”:



5.2.3. Аудит событий действий с метками

Агентское ПО “Маркер” ведет аудит действий с классифицированными документами, таких как:

- Добавление метки в неклассифицированный документ;
- Изменение классификации документа (изменение метки);
- Удаление метки из классифицированного документа;
- Открытие классифицированного документа

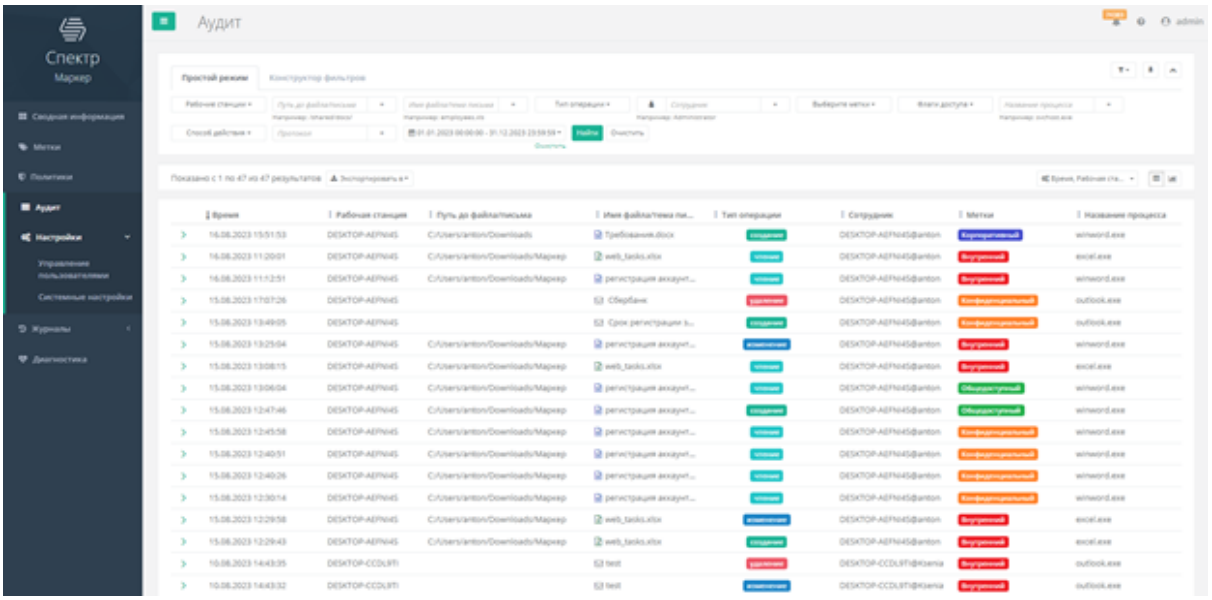
События аудита действий с классифицированными документами, такие как *Добавление/Изменение/Удаление* метки, фиксируются только при сохранении изменений в документе.

Агентское ПО “Маркер” также ведет аудит действий с классифицированными электронными письмами, таких как:

- Добавление метки в электронное письмо;
- Изменение классификации письма (изменение метки);
- Удаление метки из классифицированного письма;
- Открытие классифицированного письма;
-

События аудита действий с классифицированными письмами, такие как *Добавление/Изменение/Удаление* метки, фиксируются при отправке/сохранении электронного письма.

Результаты аудита доступны в виде журнала на вкладке “Аудит”



В журнале отображаются события действий с классифицированными документами/письмами и включаются в себя следующую информацию:

- Имя документа, с которым была проведена операция / тема электронного письма;
- Полный путь к документу (только для документов);
- Имя рабочей станции;
- Время операции (обращения) к документу/письму;
- Учетная запись пользователя, совершившего действие;
- Тип операции, производимой с документом/письмом, включающий следующие типы:
    - Чтение;
    - Изменение;
    - Удаление;
    - Создание
- Метки документа:
    - Для операций Чтения/Изменения/Создания – список всех меток в документе на момент фиксирования события;
    - Для операции Удаление – список всех удаленных меток из документа
- Статус операции;
- Способ совершения операции;
- IP-адрес совершающего операцию;
- Имя процесса, который производит операцию