Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение   
высшего профессионального образования   
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий - РТФ

**Учебно-методическое пособие по теме:   
«DLP от ESET. Развертывание системы. Возможности. Реагирование на инциденты ИБ. Как работать с зашифрованным трафиком.»**

Екатеринбург 2020

Оглавление

[Введение 3](#_Toc42656506)

[Теория 3](#_Toc42656507)

[Лабораторная работа 9](#_Toc42656508)

[Установка и предварительная настройка «Офисный контроль и DLP Safetica» 9](#_Toc42656509)

[Исходная конфигурация 13](#_Toc42656510)

[Работа с консолью управления «Офисный контроль и DLP Safetica» 15](#_Toc42656511)

[Работа основных модулей «Офисный контроль и DLP Safetica» 18](#_Toc42656512)

[Отслеживание веб-сайтов 18](#_Toc42656513)

[Категории 19](#_Toc42656514)

[Ограничение нелегитимной деятельности сотрудников с помощью модуля «Супервайзер» 20](#_Toc42656515)

[Защита от утечки конфиденциальной информации с помощью модуля DLP 22](#_Toc42656516)

[Настройка интеграции 24](#_Toc42656517)

[Список литературы: 25](#_Toc42656518)

# Введение

Многочисленные исследования утечек конфиденциальной информации свидетельствует о том, что порядка 75% утечек данных происходит из-за действий внутреннего нарушителя. Поэтому основным источником угроз для конфиденциальной информации являются сами сотрудники компании. Они имеют доступ к данным в силу своих профессиональных обязанностей. Ограничить их в доступе к этим сведениям на рабочем месте сложно, но утечка конфиденциальной информации должна пресекаться компанией. Как этого добиться? Администраторы компании могут полностью закрыть интернет, электронную почту и сменные носители, оставив тем самым пользователей совсем без доступа к внешним ресурсам. Вариант почти идеальной защищенности, за исключением того, что он никого не устраивает, кроме самих администраторов. Можно немного подобреть, и открыть доступ в интернет или к сменным носителям только «избранным» сотрудникам. Вероятность утечек уменьшится, но кто сможет гарантировать, что «избранный» сотрудник полностью лоялен компании? Казалось бы, положение безвыходное, но здесь на помощь приходят DLP-системы.

# Теория

DLP (Data Loss Prevention) система — это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети. Строится эта система на анализе потоков данных, выходящих за пределы корпоративной сети. В случае сработки определенной сигнатуры и детекта передачи конфиденциальной информации система либо блокирует такую передачу, либо посылает уведомления офицеру безопасности.

Обычно, основным способом передачи информации являются электронная почта, HTTP/HTTPS, FTP и принговые сети. Ещё один способ передачи информации, в которых шифруется весь передаваемый трафик, это VPN-тоннели.

Для контролирования сетевого трафика существует два способа внедрения DLP-систем, контролирующих сетевой трафик:

1. Использование устройства, подключенного в ”разрыв”, через которое проходит весь трафик.
2. Использование агентов, которые устанавливаются на клиентские рабочие станции.

Разработчики современных DLP-продуктов отказались от обособленной реализации защиты уровней, поскольку от утечки нужно защищать и конечные устройства, и сеть.

**Сетевой уровень контроля** при этом должен обеспечивать максимально возможный охват сетевых протоколов и сервисов. Речь идет не только о «традиционных» каналах, но и о более новых системах сетевого обмена (Instant Messengers, облачные хранилища). К сожалению, на сетевом уровне невозможно контролировать шифрованный трафик, но данная проблема в DLP-системах решена на уровне хоста.

**Контроль на хостовом уровне** позволяет решать больше задач по мониторингу и анализу. Фактически ИБ-служба получает инструмент полного контроля за действиями пользователя на рабочей станции. DLP с хостовой архитектурой позволяет отслеживать, что копируется на съёмный носитель, какие документы отправляются на печать, что набирается на клавиатуре, записывать аудиоматериалы, делать снимки экрана. На уровне конечной рабочей станции перехватывается шифрованный трафик, а для проверки открыты данные, которые обрабатываются в текущий момент и которые длительное время хранятся на ПК пользователя.

Минусы хостовой реализации в том, что системы с обширным набором функций сложнее администрировать, они более требовательны к ресурсам самой рабочей станции. Управляющий сервер регулярно обращается к модулю-«агенту» на конечном устройстве, чтобы проверить доступность и актуальность настроек. Кроме того, часть ресурсов пользовательской рабочей станции будет неизбежно «съедаться» модулем DLP. Поэтому еще на этапе подбора решения для предотвращения утечки важно обратить внимание на аппаратные требования.

Принцип разделения технологий в DLP-системах остался в прошлом. Современные программные решения для предотвращения утечек задействуют методы, которые компенсируют недостатки друг друга. Благодаря комплексному подходу конфиденциальные данные внутри периметра информационной безопасности становится более устойчивыми к угрозам.

Помимо основной задачи предотвращения утечек конфиденциальной информации у DLP-системы могут быть и второстепенные (дополнительные) задачи. К ним относятся:

* копирование передаваемых сообщений для расследования инцидентов безопасности, в будущем;
* устранение возможности оправки не только конфиденциальной информации, но и различной нежелательной (спама, оскорбительных выражений, информации эротического содержания, огромных объёмов данных и т.п.);
* фильтрация нежелательной информации при получении, а не только при отправке;
* устранения способов использования информационных ресурсов, сотрудниками, в личных целях;
* уменьшение трафика, оптимизация нагрузки каналов;
* контроль рабочего времени сотрудников.

Проведём сравнительный анализ различных DLP систем представленных сейчас на рынке:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Параметры | SecurIT | InfoWatch | Symantec | SearchInform | FalconGaze |
| Название системы | ZGate | TrafficMonitor | DataLossPrevention | Контур безопасности | SecureTower |
| Модульность системы | Да | Нет | Нет | Да | Нет |
| Места установки | На сервер+ZLock на клиентские ПК | Сервер, клиент | Сервер, клиент | Сервер, клиент | Сервер, клиент |
| Наличие сертификатов и лицензий | ФСТЭК НДВ 3 и ОУД4 | ФСТЭК НДВ 4 и ИСПДн 1, Газпромсерт, Аккредитация ЦБ, сертификат совместимости eToken | ФСТЭК НДВ 4 | ФСТЭК НДВ 4 | ФСТЭК НДВ 4 и ИСПДн 2 |
| Лицензирование | Почтовые ящики, рабочие места | Каналы перехвата, технологии анализа | n/a | Сервер, mail, IM, Skype, Print, device, HTTP, FTP | Рабочее место |
| Роли | Любое количество | Несколько | Любое количество | Любое количество | Администратор системы, офицер безопасности |
| Контроль IM | Да | Да | Да | Да | Да |
| Контроль HTTP/HTTPS, FTP | Да | Да | Да | Да | Да |
| Контроль Skype | Текст | Текст | Нет | Да | Да |
| Контроль E-mail | Да | Да | Да | Да | Да |
| Социальные сети и блоги | Да | Да | Да | Да | Да |
| Контроль подключаемых внешних устройств | При покупке Zlock | Да | Да | Да | Нет |
| Контроль портов | USB,COM,LPT, Wi-Fi, Bluetooth | USB,COM,LPT, Wi-Fi, Bluetooth | USB,COM,LPT, Wi-Fi, Bluetooth | USB, LPT | USB, LPT |
| Блокируемые протоколы | HTTP, HTTPS, SMTP, OSCAR | HTTP, HTTPS, FTP, FTP over HTTP, FTPS, SMTP, SMTP/S, ESMTP, POP3, POP3S, IMAP4, IMAP4S | SMTP, HTTP, HTTPS FTP, Yahoo Messenger, MSN Messenger, AIM, AIM Pro Messenger, MSN Messenger, AIM, AIM Pro Messenger, MSN Messenger, AIM, AIM Pro | SMTP, POP3, MAPI, IMAP, HTTP,FTP, ICQ, Jabber | HTTP, HTTPS, FTP, FTTPS, Вся почта и IM |
| Анализ по словарю | Да | Да | Да | Да | Да |
| Лингвистический анализ | Да | Да+БКФ | Нет | да | Да |
| Анализ транслита | Да | Да | Нет | n/a | n/a |
| Анализ архивов | Да | Да | Да | Да | Да |
| Анализ рисунков | Да | Да | Да | Да | Нет |
| Предустановленные шаблоны фильтрации | Да | Да | Да | Да | Да |
| Задержка отправки подозрительных сообщений | Да, ОБ принимает решение | Да, ОБ принимает решение | Да, пользователь объясняет причину отправки, инцидент фиксируется | n/a | Нет, только информирование офицера ИБ |
| Логирование действий администраторов системы | Да | Да | Да | n/a | В случае утановки агента на РМ администратора |
| Режим установки агентов | Открытый | n/a | n/a | n/a | Тайный/Открытый |
| Защита агентов от выключения | Да | Да | Да | Да | Да |
| Запись отчетов в локальное хранилище в случае недоступности сервера | Да | Да | Да | Да | Да |
| Просмотр истории инцедентов | Да | Да | Да | Да | Да |
| Режимы оповещений | Консоль, почта, графики | Консоль, почта | Консоль, почта, графики | Консоль, почта, графики | Консоль, почта, графики |
| Возможность тестирования продукта на серверах разработчика | нет | нет | Да | нет | на сервере дистрибьютора |
| Возможность получения демо-версии для тестирования внутри организации | ± | ± | нет | ± | Да, 1 месяц |
| Цена для компании 250 ПК | 2 500 000р. | n/a | n/a | 3 300 000- 5 400 000 р. | 1 500 000 |

# Лабораторная работа

Подготовка к выполнению лабораторной работы:

Лабораторная работа будет выполняться на основе DLP от ESET.

«Офисный контроль и DLP Safetica» поддерживает автоматический и «ручной» варианты установки, а также извлечение компонентов в случае необходимости. Автоматическая установка предназначена для тестирования или для небольшого количества клиентов «Офисный контроль и DLP Safetica», установленных на конечных точках.

1. Ознакомьтесь с теоретическим материалом

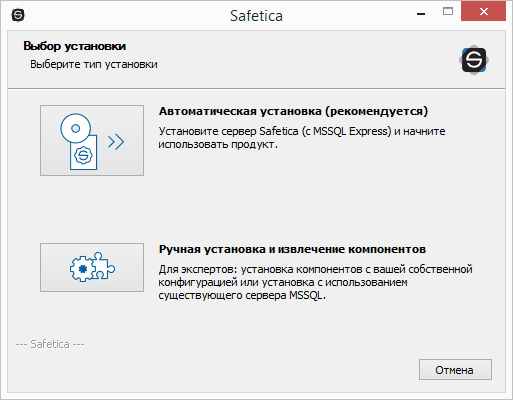
## Установка и предварительная настройка «Офисный контроль и DLP Safetica»

1. Перед установкой выполните следующие шаги:
   1. Проверьте, выполняются ли требования к аппаратному и программному обеспечению для всех трех компонентов Safetica.
   2. Проанализируйте свою корпоративную сеть:

* Решите, на какие компьютеры вы будете устанавливать сервер. При принятии этого решения учитывайте следующие аспекты:
  1. Компьютер с сервером Safetica должен иметь возможность подключения к серверу SQL, на котором будут храниться основные базы данных.
  2. С учетом количества одновременно подключаемых клиентов и типа используемого сервера базы данных, рассчитайте количество необходимых серверов для вашей среды. Допустимое количество клиентов, подключенных к одному серверу, ограничивается возможностями базы данных SQL, в которой этот сервер хранит данные (подробнее см. ниже).
* Решите, на какие компьютеры в вашей сети вы будете устанавливать консоль. Компьютеры с установленной консолью должны иметь возможность подключения ко всем серверам, которые вы собираетесь администрировать с помощью консоли управления.
* Решите, на какие компьютеры в вашей сети вы будете устанавливать агент загрузчика.
* Компьютер с агентом загрузчика должен иметь подключение хотя бы к одному серверу Safetica.
* Решите, на какие компьютеры в вашей сети вы будете устанавливать

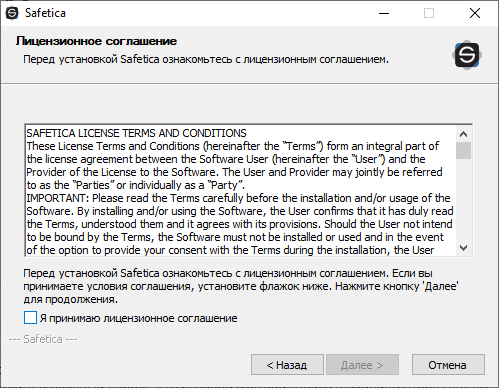
1. Установка

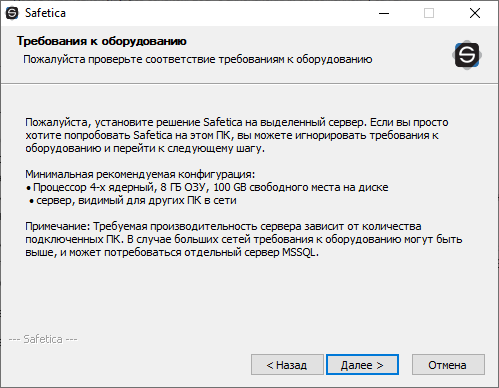
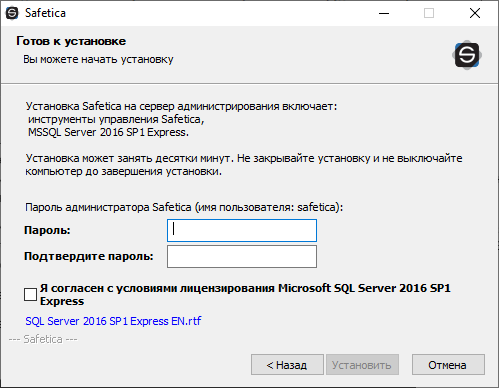
«Офисный контроль и DLP Safetica» поддерживает автоматический и «ручной» варианты установки, а также извлечение компонентов в случае необходимости. Автоматическая установка предназначена для тестирования или для небольшого количества клиентов «Офисный контроль и DLP Safetica», установленных на конечных точках.



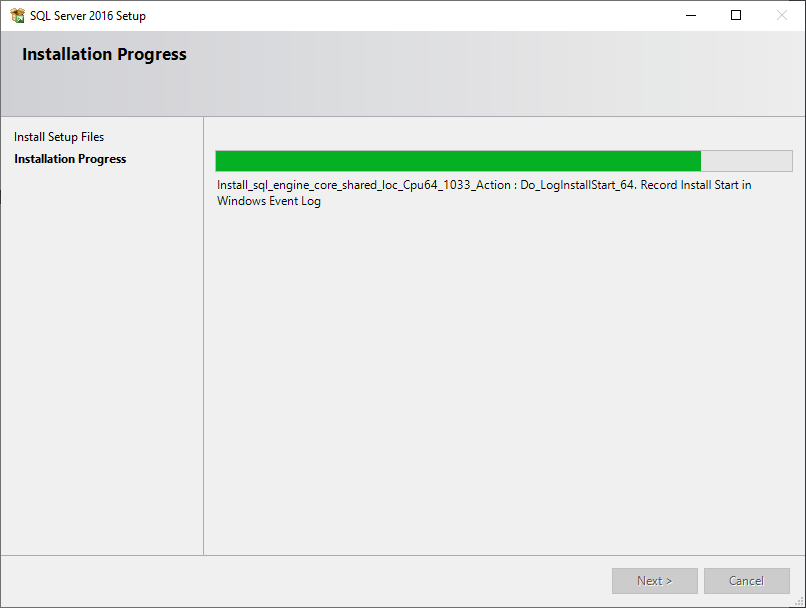
После запуска установщика Safetica выполните следующие действия:

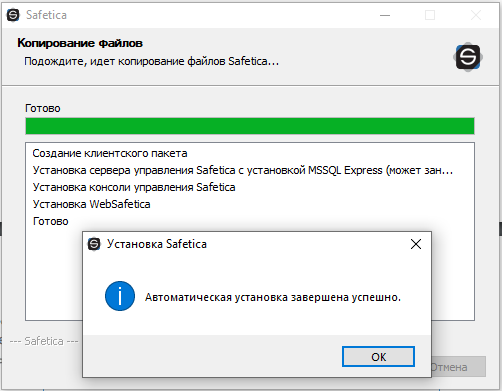
1. Нажмите на вариант Автоматическая установка и примите условия лицензионного соглашения.



1. После этого вы увидите требования к аппаратному обеспечению. Прочтите их и продолжайте процесс установки. 
2. Введите надежный пароль для базовой учетной записи администратора safetica. Примите условия лицензионного соглашения сервера SQL и запустите установку, нажав на кнопку Установить. 

Примечание. WebSafetica использует веб-сервер Microsoft IIS и порты 80 и 443. Убедитесь, что на компьютере не запущено приложение, которое может заблокировать порты 80 или 443, либо настройте для IIS другие порты после установки.



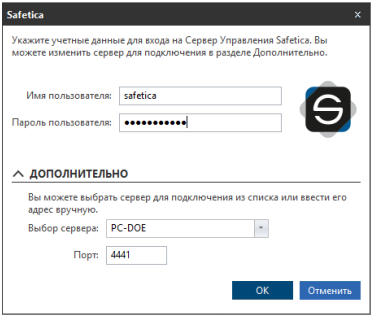


1. Убедиться, что консоль установлена.

## Исходная конфигурация

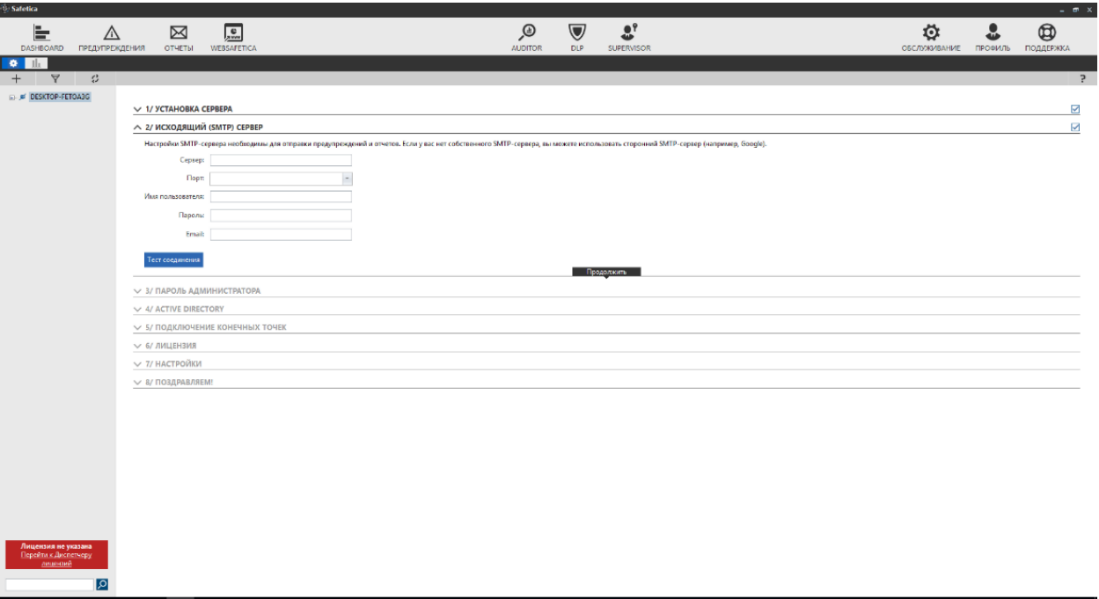
После успешной установки консоли и сервера нужно правильно настроить всю систему до начала установки агента загрузчика и клиента на конечных компьютерах. Все действия по администрированию и настройке выполняются через консоль.

1. Запустите консоль. В диалоговом окне введите реквизиты служебной учетной записи, чтобы войти на сервер. Имя служебной учетной записи — safetica, а пароль, который был поставлен при установке. В расширенных настройках введите адрес или имя сервера, на котором установлен сервер. Используйте порт по умолчанию 4441 для входа в консоль на сервере. Нажмите OK для подтверждения.

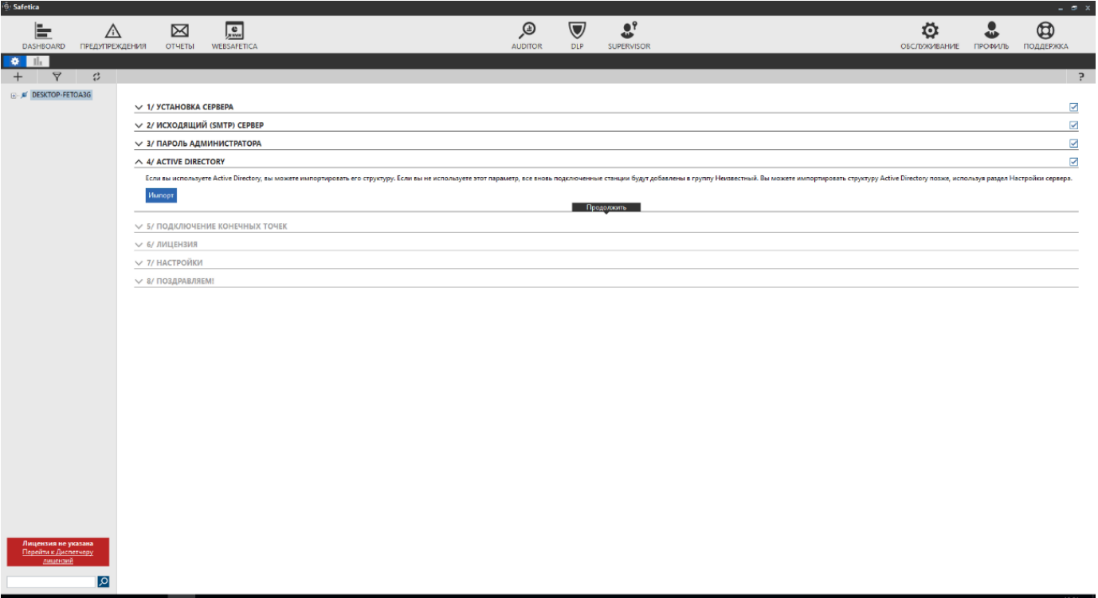


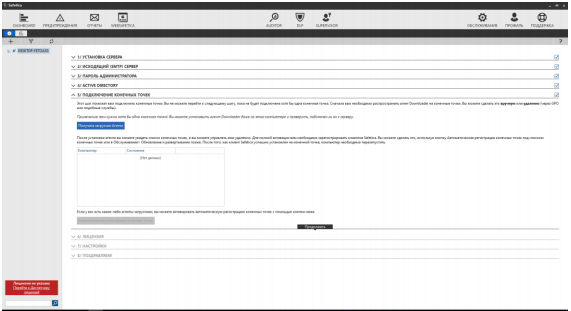
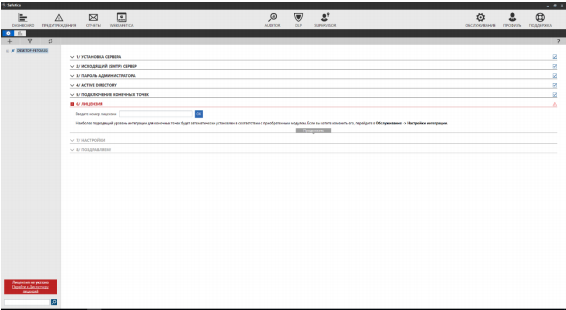
1. В Safetica откроется мастер первичной настройки. Настройки сервера Safetica и сервера SMTP для отправки электронной почты выполняются в процессе установки. Если все пройдет нормально, мастер откроет дерево элементов. Установите новый пароль к служебной учетной записи Safetica для входа в консоль Safetica. Нажмите Далее.

Примечание. Служебная учетная запись имеет все права для работы с функциями и настройками Safetica. Данные для входа в эту учетную запись следует хранить в надежном месте. Если вы хотите предоставить другим пользователям доступ к Safetica, создайте для них новую учетную запись на вкладке Обслуживание -> Управление доступом -> Добавить аккаунт.



1. Вы можете импортировать в Safetica всю корпоративную структуру из Active Directory. Выполнить импорт из Active Directory позднее, выбрав Профиль -> Настройки сервера в разделе Настройки соединения с базой данных.

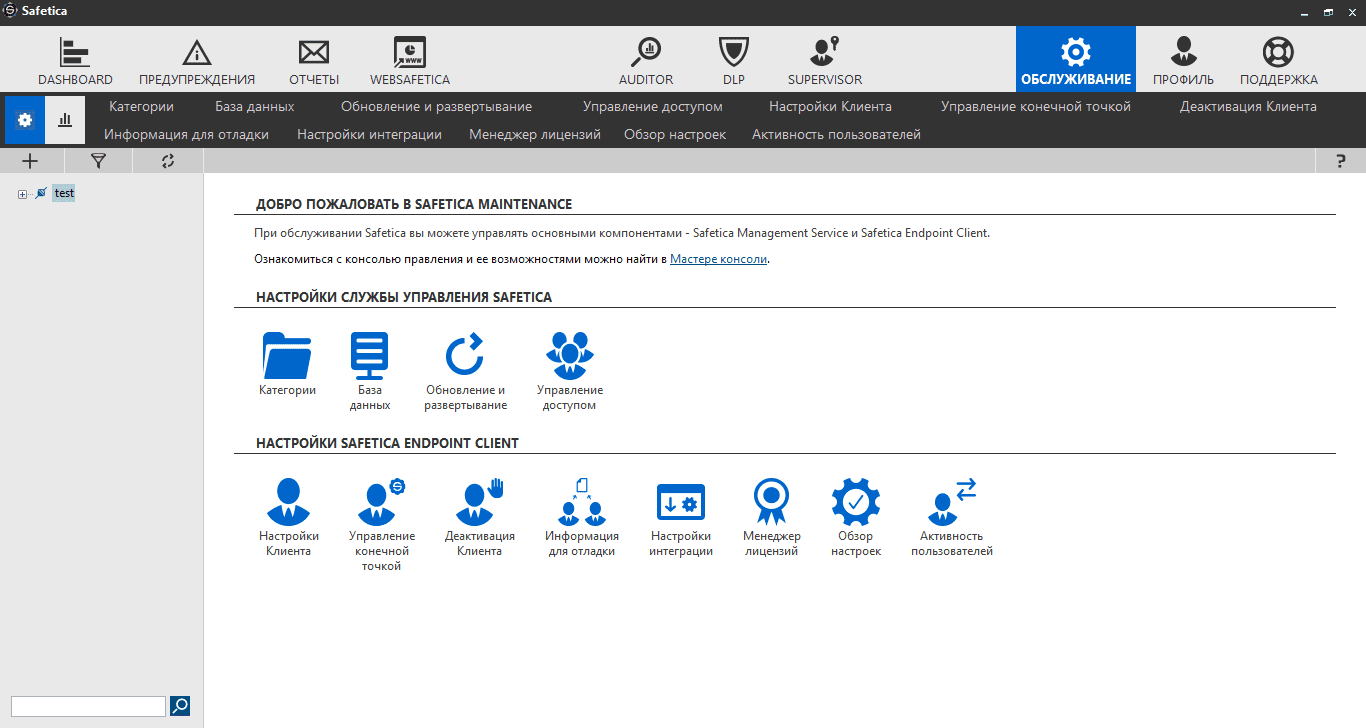


1. Этот шаг поможет вам установить агент загрузчика на конечных компьютерах, чтобы их можно было подключить к Safetica. Нажав Получить пакет Агента, вы запустите создание агента загрузчика, который затем можно будет установить на всех рабочих станциях. Установить агент можно двумя способами:
   * удаленная (пакетная) установка;
   * ручная установка.
2. После установки агентов загрузчика вы можете автоматически установить и активировать клиентов Safetica, нажав Автоматическая регистраций конечных компьютеров. Задачей установки клиента можно управлять из меню Консоль -> Обслуживание -> Управление конечной точкой.
3. На этом шаге введите лицензионный ключ Safetica. Лицензионный ключ можно ввести позднее, открыв меню Обслуживание -> Менеджер лицензий.8
4. На последнем шаге работы мастера вы можете выбрать предустановленные функции Safetica или настроить их вручную.
5. Выйдите из мастера, нажав кнопку Включить защиту данных

## Работа с консолью управления «Офисный контроль и DLP Safetica»

«Офисный контроль и DLP Safetica» позволяет контролировать работу своих основных компонентов из единого веб-интерфейса — консоли управления. Она дает возможность конфигурировать работу основных модулей, настраивать службы управления «Офисный контроль и DLP Safetica» и администрировать клиенты, установленные на конечных точках. Консоль работает в двух режимах: настройки и визуализации. В режиме визуализации, в зависимости от модуля и функции, представляются записанные данные и графики, связанные с выбранным пользователем или группой. Поддерживается создание собственных макетов диаграмм, столбцов и фильтров, а также экспорт отображаемых графиков и диаграмм в PDF и XLS.

1. Открыть окно с основными элементами консоли управления «Офисный контроль и DLP Safetica»

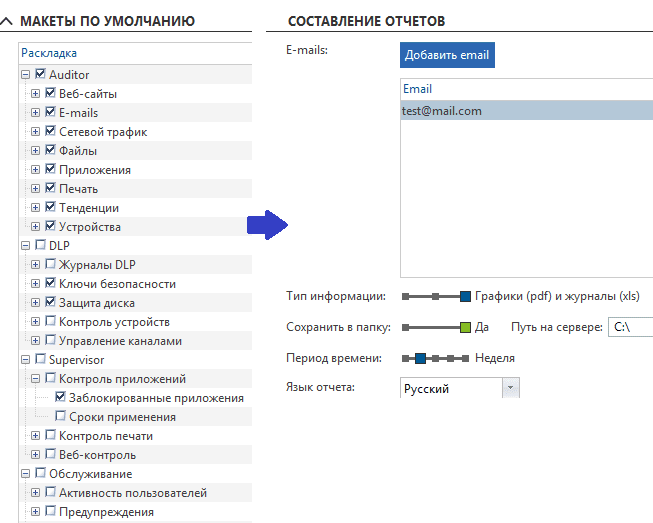


1. Откройте раздел Обновления и развертывания. Изучите возможности управления обновлениями клиентов и сервера.
2. Откройте раздел Базы данных. Изучите возможности резервного копирования, выбора и удаления отслеживаемых данных. Сделайте выводы о возможностях данного раздела
3. Откройте раздел Управлениями доступами. Измените права доступа одного из клиентов. Варианты учётных записей:

* Администратор - имеет полный доступ ко всем функциям и настройкам
* Диспетчер - способен видеть записи всех функций, но не вправе вносить изменения в конфигурацию
* Пользователь - может работать с конкретными функциями и параметрами, которые ему назначил администратор

Настройте учетную запись администратора по своему усмотрению

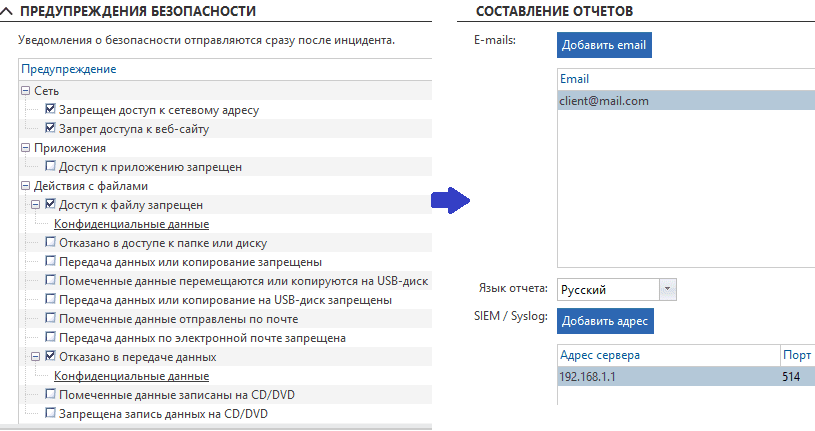
1. Открыть раздел генерации отчёта по деятельности сотрудника.



1. Настройте отчёт.

Если на рабочей станции, подключенной к «Офисный контроль и DLP Safetica», сработало определенное правило, то продукт должен вывести пользователю информационное сообщение, а также составить отчет и выслать его на указанную почту либо отправить в формате SIEM или Syslog на сервер. В консоли управления для этого поддерживаются триггеры действий, которые основываются на записях активности пользователя, что позволяет запускать команды на рабочей станции сотрудника или инициировать запуск скриптов с конкретными аргументами и в выбранной папке.

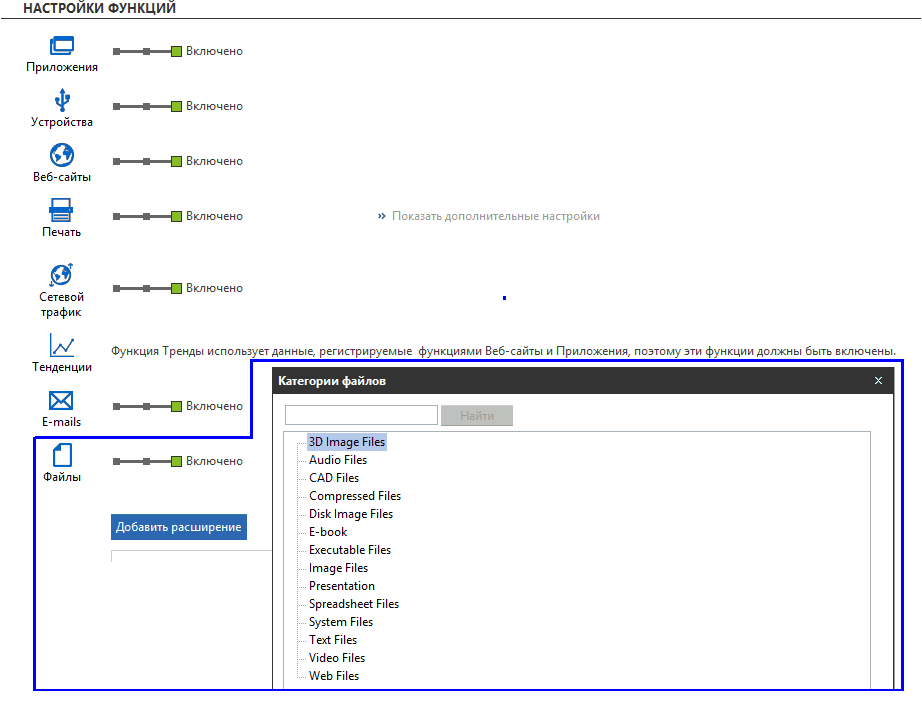
1. Настройте триггеры действий в консоли управления.



## Работа основных модулей «Офисный контроль и DLP Safetica»

**Выявление нестандартного поведения сотрудников с помощью модуля «Аудитор»**

1. Откройте настройки функций модуля **«Аудитор»**



1. Включите отслеживание:

* Приложений
* Устройств
* Веб-сайтов
* Печати
* Почты
* Файлов
* Тенденции

1. Перейдите в раздел тенденции и проанализируйте увиденное.
2. С помощью раздела Устройства наглядно пронаблюдайте, как система отслеживает подключение USB-накопителей. Убедитесь в том, что «Аудитор» позволяет отследить все подобные подключения с детализацией по приложениям, типу устройства и интерфейса, вендору и описанию.

## Отслеживание веб-сайтов

Auditor также позволяет надежно блокировать доступ к веб-сайтам, доступ к которым осуществляется по защищенному порту HTTPS.

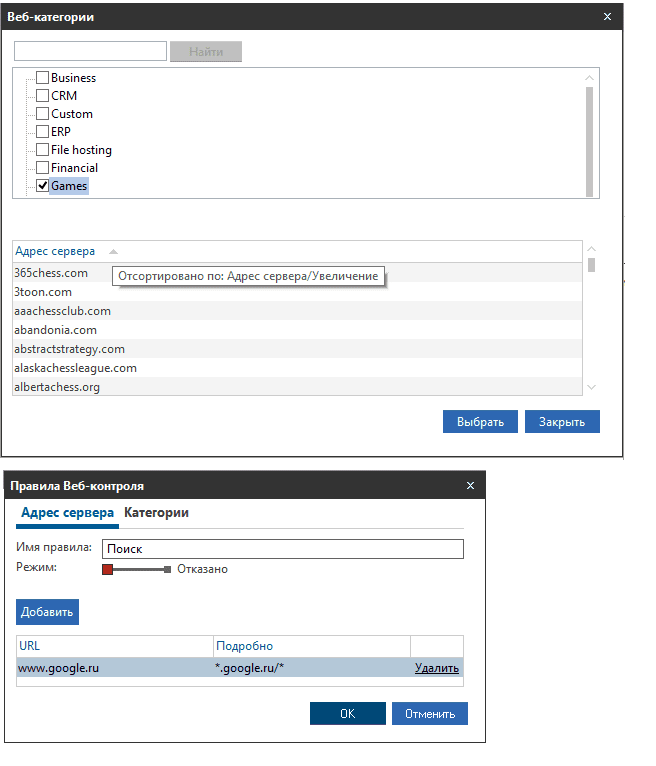
В разделе Supervisor -> Веб-контроль вы можете управлять веб-сайтами, которые помещают пользователи.

В режиме настройки консоли вы можете отключить или включить эту функцию, используя полосу прокрутки в заголовке экрана. Вы можете выбрать для правил действие по умолчанию:

* Разрешено — при этом будет разрешен доступ к веб-сайтам, которых нет в списке.
* Наследовать — настройки наследуются от родительской группы.
* Отказано — доступ к веб-сайтам, не указанным в списке, будет запрещен.

Вы можете удалить правило из списка с помощью кнопки Удалить. Редактировать выбранное правило можно с помощью кнопки Изменить.

1. Создайте правило запрещающее посещение сайта ВКонтакте и YouTube
2. Проверьте работает ли настроенное вами правило
3. Откройте раздел “Супервайзер”
4. В разделе настройки веб-контроля установите для сотрудника ограничения на посещение веб-сайтов по вашему выбору.



## Категории

Safetica содержит готовые категории веб-сайтов, приложений и расширений. Категории используются в разных функциях Safetica для удобства ориентации в записанных данных и настройки разных политик безопасности. В таблице категорий можно обновлять базу данных категорий, редактировать имеющиеся и создавать свои собственные категории приложений или веб-сайтов. Настройки категорий доступны в меню Обслуживание -> Категории.

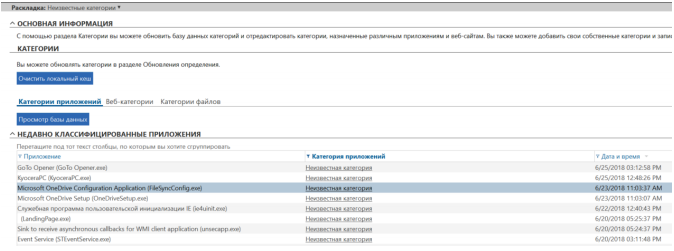
В верхней части экрана есть кнопка с надписью *“Очистить локальный кэш”*. Она очищает локальный кэш с информацией о распределении приложений и веб-сайтов по категориям на всех рабочих станциях, где установлен клиент. Это действие ускоряет распространение новых данных о категориях приложений и/или веб-сайтов, измененных через консоль. Мы советуем использовать эту опцию только в исключительных и действительно срочных случаях. Примечание. Удаление кэша категорий будет выполняться только на тех клиентах, которые подключены к серверу и управляются через запущенную консоль. Время выполнения операции зависит от того, когда отдельные клиенты загрузят актуальные настройки. В центральной части этого экрана представлены следующие настройки для каждой категории:

* Веб-категории — доступ к управлению категориями веб-сайтов. Здесь вы можете добавлять свои категории и веб-сайты.
* Категория приложений — доступ к управлению категориями приложений. Здесь вы можете добавлять свои категории и приложения.
* Категории файлов — доступ к управлению категориями расширений. Здесь вы можете добавлять свои категории и расширения.

1. Выберите из дерева серверов тот, на котором вы хотите управлять категориями. Вы можете отобразить категории, нажав на кнопку Просмотр базы данных. Если вы отметите несколько экземпляров в дереве, после нажатия кнопки будут отображаться только те категории, которые сделаны общими для выбранных серверов.

В нижней части находится таблица со списком последних категоризированных вебсайтов или приложений в соответствии с выбранной вкладкой. Можно вручную изменить категорию, нажав на категорию в каждой записи.

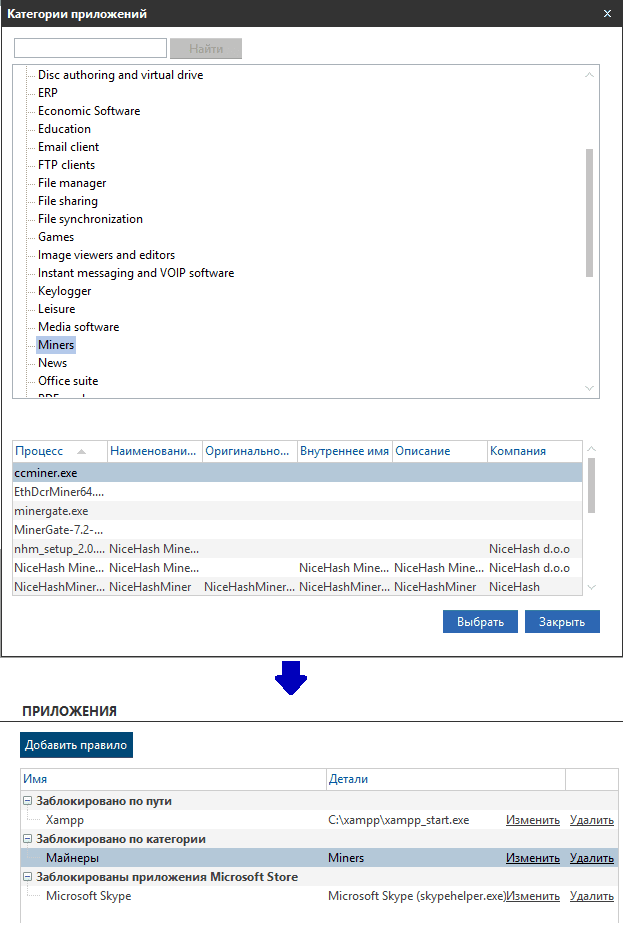
Примечание. Также вы можете использовать категоризацию в WebSafetica



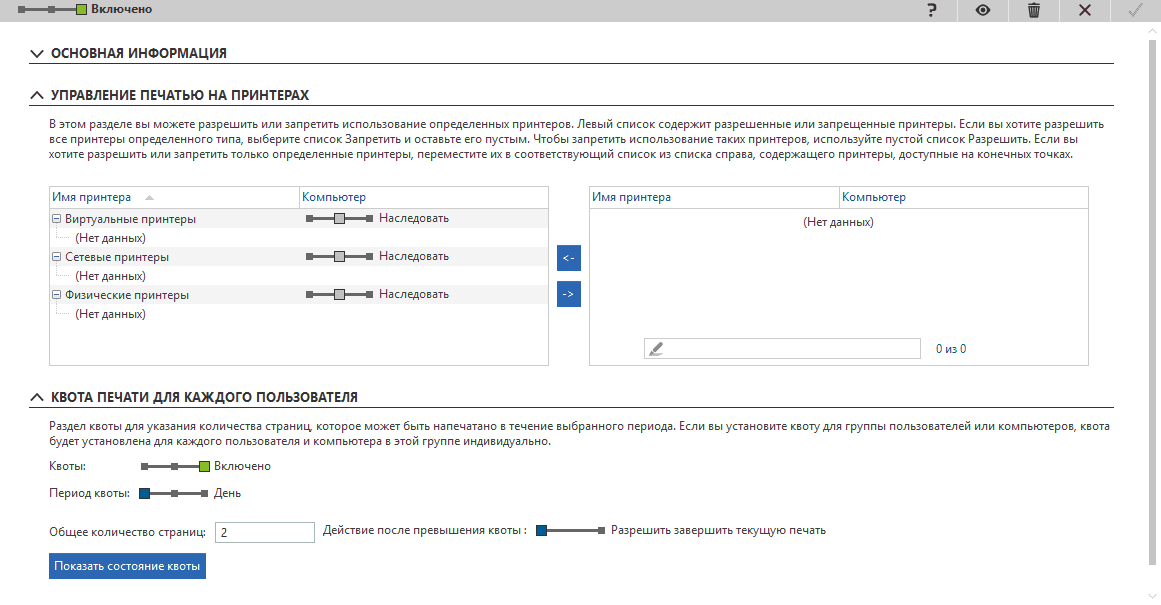
1. Добавьте свою веб-категорию запрещающую доступ к вредоносным сайтам (не менее 3) и создайте для неё правило.
2. Проверьте работу правил с категориями.

## Ограничение нелегитимной деятельности сотрудников с помощью модуля «Супервайзер»

1. Перейдите в раздел настроек контроля приложений.
2. Настройте правило для приложений. Правила задаются посредством указания категории или системного пути; возможен также выбор прикладных программ, полученных из магазина Microsoft.



1. Откройте раздел настройки контроля печати.
2. Установите на каких принтерах может печатать сотрудник и установите квоту на печать.

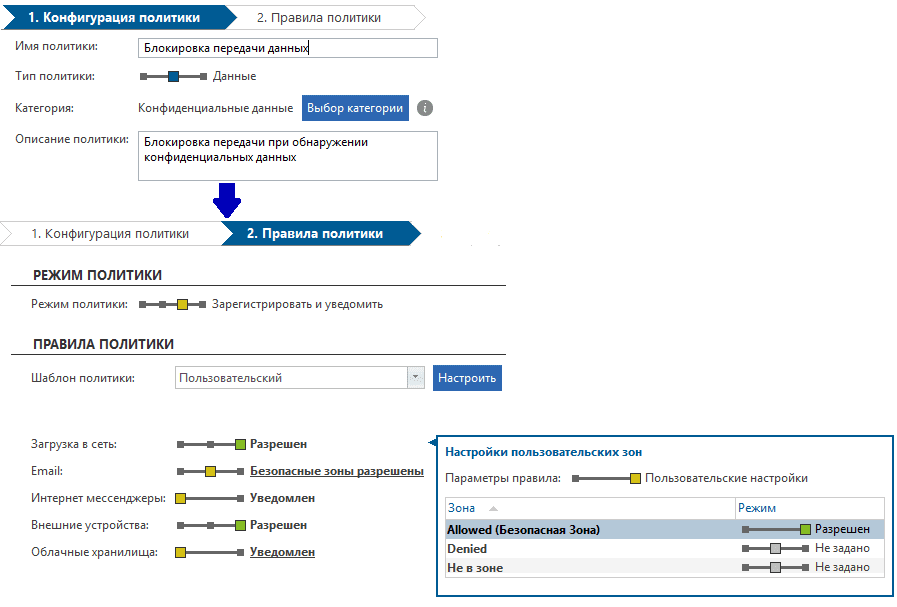


## Защита от утечки конфиденциальной информации с помощью модуля DLP

1. Откройте раздел создания политики безопасности.

Важным этапом конфигурации модуля является выбор режима, в котором будет работать политика DLP, поскольку он определяет характер ее реагирования на события безопасности. Каждый из возможных режимов является сочетанием трех функций (протоколирование, уведомление и блокировка), которые могут быть отключены или активированы.

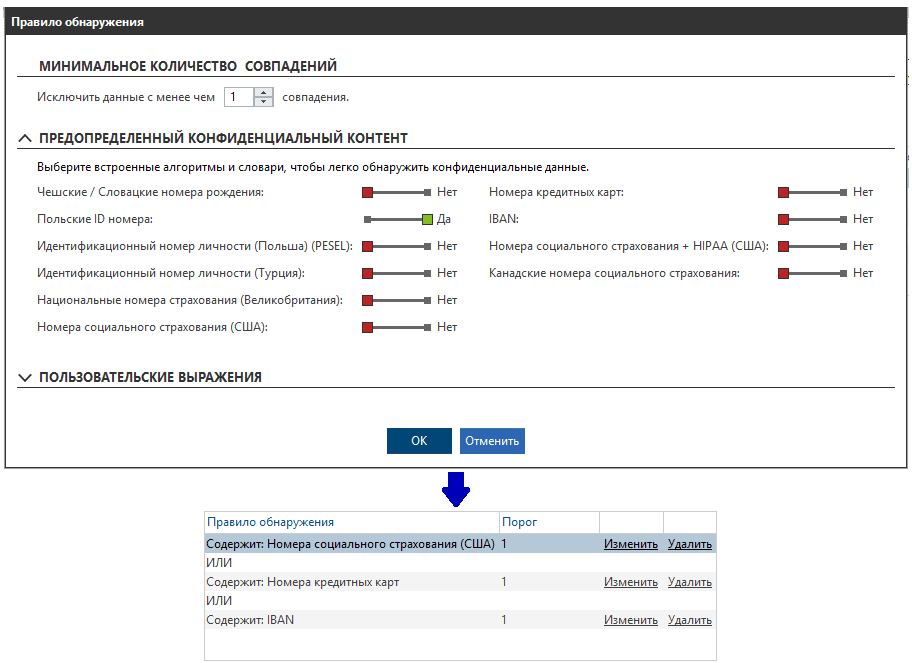
1. Задайте желаемую политику безопасности.



1. Перейдите в раздел настройки категории данных DLP

Категории данных предназначены для разделения файлов на группы в зависимости от того, кто может с ними работать. Категоризация основана на трех способах: выражения, метаданные и метки для файлов. Самым простым вариантом является использование словарей вместе с регулярными выражениями.

1. Настройте категории данных.

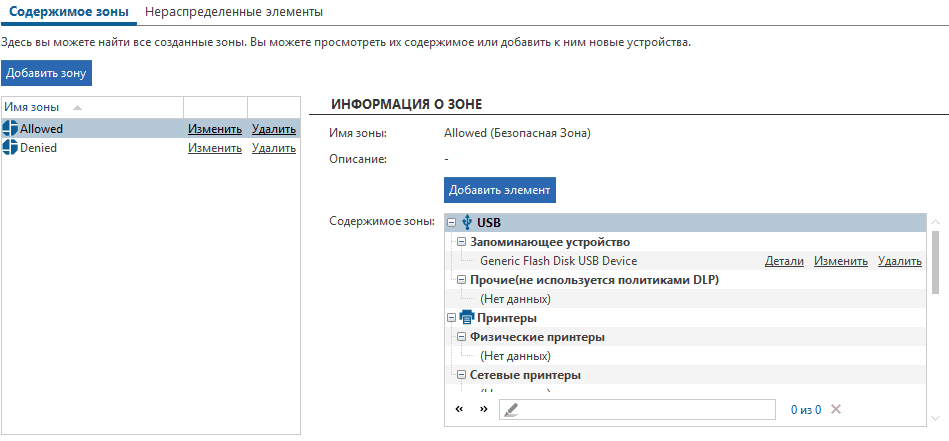


1. Откройте раздел настройки зон в модуле DLP.

Зоны DLP и контроль устройств нужны для гибкой конфигурации групп внешнего аппаратного обеспечения, принтеров, IP-адресов, сетевых путей, которые могут администрироваться различными функциями DLP, а также для управления свойствами устройств. Зоны разделяются на безопасные и небезопасные. Безопасные зоны, как правило, используются для настройки доверенной среды компании. В зону могут быть включены:

* внешние устройства, которые добавляются автоматически (когда консоль управления сама видит их) или вручную, когда необходимо ввести информацию о производителе в соответствующие поля;
* IP-адреса, маски подсети или диапазоны IP-адресов;
* сетевые пути;
* адреса электронной почты и почтовые домены;
* принтеры, сетевые и физические;
* веб-адреса, которые могут быть заданы в виде отдельного URL (\*.google.ru) или доменной зоны (.com).

1. Настройте безопасную зону с помощью модуля DLP.



## Настройка интеграции

Настройки интеграции определяют поведение Safetica на рабочих станциях. Настройки интеграции находятся на консоли в меню Обслуживание -> Настройки интеграции.

1. Зайдите в настройки интеграции и активируйте интеграцию в SSL/TLS

Интеграция в SSL/TLS - если интеграция активна, Safetica сможет контролировать все зашифрованные коммуникации SSL/TLS и/или вмешиваться в такие коммуникации с целью обеспечения безопасности. Это может произойти, например, в принудительной политике безопасности.

Safetica предоставляет менеджерам четкую статистику наиболее посещаемых страниц и времени, потраченного на их просмотр. Страницы классифицируются в соответствии с категорией, количеством открытий и уровнем производительности. Поддерживаются все основные веб-браузеры (Internet Explorer, Edge, Chrome, Opera, Firefox). Можно анализировать даже зашифрованные соединения HTTPS. Функцию мониторинга веб-сайтов можно найти в модуле Auditor -> Веб-сайты.

1. На вкладке Auditor -> Настройки функций включите функцию мониторинга веб-сайтов.
2. Проверьте работу мониторинга. Откройте любой сайт с зашифрованным соединением, изучите результат. Сделайте выводы.

# Источники:

1. Системы защиты от утечек (DLP). <http://www.infokube.ru/index.php/products/categories/category/dlp>
2. «Сравнение систем защиты от утечек (DLP)». Александр Панасенко.
3. “Офисный контроль и DLP SAFETICA. Safetica полная документация”
4. Шихов Е. Обзор DLP-систем на мировом и российском рынке. Статья 8 августа 2016 (электронный ресурс) <https://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014#part4>
5. Системы DLP - Who? What? Where? How? <http://www.topsbi.ru/default.asp?artID=1675>