КИБЕРПРОТЕКТ

КИБЕР Протего

Версия 10.2.1

Руководство пользователя Cyber Protego Discovery

Редакция: 30.05.2024

Заявление об авторских правах

Содержание

Краткий обзор Cyber Protego Discovery

Представляем Cyber Protego Discovery

Cyber Protego Discovery еще дальше расширяет возможности Cyber Protego, помогая сетевым администраторам и специалистам по безопасности обнаруживать определенные типы контента, хранящиеся внутри и за пределами корпоративной сети. Обнаружение нежелательного контента является очень важным, когда вы стараетесь защитить интеллектуальную собственность компании, контролировать деятельность сотрудников и администрировать компьютерные сети.

Cyber Protego Discovery – это серверный компонент, который является составной частью Cyber Protego Search and Discovery Server. Cyber Protego Discovery предназначен для сканирования рабочих станций пользователей и систем хранения информации, расположенных как внутри, так и за пределами корпоративной сети компании, и обнаружения определенных типов контента в соответствии с заданными правилами. Администратор может назначить правила, согласно которым будет вестись поиск контента, недопустимого в корпоративной сети.

Cyber Protego Discovery способен выполнять аудит всех типов контента, хранящегося на конкретной рабочей станции и системе хранения данных. Исходя из заданного контекста безопасности, эта возможность позволяет сетевым администраторам и специалистам ИТ-отдела производить комплексный аудит контента, хранящегося на локальных ресурсах организации.

Описание Cyber Protego Discovery

Cyber Protego Discovery предназначен для обнаружения определенного контента, размещенного на компьютерах и устройствах хранения данных, подключенных к локальной сети, включая локальные папки синхронизации облачных агентов файлового обмена. При использовании совместно с Cyber Protego компонент Cyber Protego Discovery существенно повышает возможности контентно-зависимых правил. Используя Cyber Protego Discovery, можно не только выявлять различную информацию, но и выполнять ряд действий, направленных на предоставление или запрет доступа к этой информации, оперативно предупреждать администратора, удалять или зашифровывать выявленный контент, либо уведомлять пользователя компьютера о нарушениях политики безопасности.

Cyber Protego Discovery позволяет обнаруживать данные, основываясь на технологии определения реального типа файлов, позволяет использовать шаблоны регулярных выражений с числовыми и булевыми порогами срабатывания, а также по ключевым словам. Распознавая более восьмидесяти форматов файлов и типов данных, Cyber Protego Discovery извлекает и отфильтровывает содержимое данных, хранимых на локальных жестких дисках рабочих станций, в локальных папках синхронизации облачных агентов файлового обмена, подключаемых plug-n-play устройствах хранения данных и NAS-серверах, подключенных к локальной сети. С помощью Cyber Protego Discovery можно существенно сузить поиск, ограничившись только теми данными, которые значимы для аудита информационной безопасности, расследования инцидентов и криминалистической экспертизы.

Возможности и преимущества

Основные возможности и преимущества Cyber Protego Discovery:

Обнаружение, основанное на контентном анализе. Возможность обнаруживать информацию и автоматически выполнять определенные действия, основываясь на реальном типе данных и актуальном содержимом. Обнаружение, основанное на контентном анализе данных, может выявлять множество различного рода данных, даже если файлы были переименованы либо было изменено их расширение. Таким образом, можно выявлять ценные корпоративные данные, при этом получая немедленное тревожное алерт, удаляя данные из точки хранения или изменяя права доступа к данным.

Обнаружение документов на основе классификации контента. Возможность обнаруживать документы и автоматически выполнять определенные действия, основываясь на следующих признаках:

- Цифровые отпечатки конфиденциальных документов, которые снимаются и хранятся на сервере Cyber Protego Management Server. Обнаружение на основе отпечатков позволяет идентифицировать полные копии, а также фрагменты документов, даже если документ был изменен.
- Классификационные метки сторонних продуктов, таких как приложения Boldon James Classifier, в которых атрибуты документа устанавливаются в соответствии с уровнем его секретности.

Обнаружение документов в Elasticsearch. Возможность обнаруживать интересующие документы в Elasticsearch - распределенной программной системе, обеспечивающей индексирование и поиск различных типов данных в реальном времени. Cyber Protego Discovery запрашивает поиск документов в Elasticsearch, сопоставляет результаты поиска с правилами обнаружения, а затем отправляет алерта, протоколирует события и создает отчеты по результатам обнаружения.

Поддержка множества типов файлов и данных. Позволяет анализировать содержимое файлов и данных следующих типов: Adobe Acrobat (включая зашифрованные файлы, если шифрование файла выполнено одним из следующих алгоритмов: 40-bit RC4, 128-bit RC4, 128-bit AES и 256-bit AES, и при этом разрешения, установленные на файл, не запрещают извлечение текста) (*.pdf), Adobe Framemaker MIF (*.mif), Ami Pro (*.sam), Ansi-текст (*.txt), ASCII-текст, ASF-файлы (только метаданные) (*.asf) , AutoCAD (*.dwg, *.dxf), CSV (значения, разделённые запятыми) (*.csv), DBF (*.dbf), EBCDIC, EML (сохраненные в Outlook Express письма) (*.eml), Enhanced Metafile Format (*.emf), Eudora MBX-файлы (*.mbx), Flash (*.swf), GZIP (*.gz), HTML (*.htm, *.html), iCalendar (*.ics), Ichitaro (версия 5 и выше) (*.jtd, *.jbw), JPEG (*.jpg), Lotus 1-2-3 (*.123, *.wk?), почтовые архивы MBOX (включая Thunderbird) (*.mbx), MHT-файлы (HTML-архивы, сохраненные Internet Explorer) (*.mht), MIME-сообщения (включая вложения), MSG (сохраненные в Outlook письма) (*.msg), Microsoft Access MDB-файлы (включая Access 2007 и Access 2010) (*.mdb, *.accdb), Microsoft Document Imaging (*.mdi), Microsoft Excel (*.xls), Microsoft Excel 2003 XML (*.xml), Microsoft Excel 2007, 2010 и 2013 (*.xlsx), Microsoft OneNote 2007, 2010 и 2013 (*.one), файлы Microsoft Outlook (*.PST), сообщения, заметки, контакты, встречи и задачи календаря Microsoft Outlook/Exchange, хранилища сообщений Microsoft Outlook Express 5 и 6 (*.dbx), Microsoft PowerPoint (*.ppt), Microsoft

PowerPoint 2007, 2010 и 2013 (*.pptx), Microsoft Rich Text Format (*.rtf), Microsoft Searchable Tiff (*.tiff), Microsoft Visio (*.vsd, *.vst, *.vss, *.vdw, *.vsdx, *.vssx, *.vstx, *.vsdm, *.vssm, *.vstm), Microsoft Word for DOS (*.doc), Microsoft Word для Windows (*.doc), Microsoft Word 2003 XML (*.xml), Microsoft Word 2007, 2010 и 2013 (*.docx), Microsoft Works (*.wks), MP3 (только метаданные) (*.mp3), Multimate Advantage II (*.dox), Multimate версии 4 (*.doc), документы, таблицы и презентации OpenOffice версий 1, 2 и 3 (включает OASIS Open Document Format for Office Applications) (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf), Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw), QuickTime (*.mov, *.m4a, *.m4v), RAR (*.rar), TAR (*.tar), TIFF (только метаданные) (*.tif), TNEF (winmail.dat), Treepad HJT-файлы (*.hjt), Unicode (UCS16, формат Mac или Windows, UTF-8), Visio XML-файлы (*.vdx), Windows Metafile Format (*.wmf), WMA-файлы (только метаданные) (*.wma), WMV-файлы (только метаданные) (*.wmv), WordPerfect 4.2 (*.wpd, *.wpf), WordPerfect (версия 5.0 и выше) (*.wpd, *.wpf), WordStar version 1, 2, 3 (*.ws), WordStar версии 4, 5, 6 (*.ws), WordStar 2000, Write (*.wri), XBase (включая FoxPro, dBase и другие XBase-совместимые форматы) (*.dbf), XML (*.xml), XML Paper Specification (*.xps), XSL, XyWrite, ZIP (*.zip), а также PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, EMF Spooled Files и GDI Printing (ZjStream).

Примечание

Анализ контента документов AutoCAD (.dwg, .dxf) поддерживается на клиентских компьютерах под управлением Windows 7 или более поздних версий ОС.

Непрерывная защита. Возможность применения контентно-зависимых политик безопасности ко всей сети на периодической основе посредством заданных расписаний сканирования.

Различные методы обнаружения контента. Позволяют обнаруживать и идентифицировать критически важную для организации информацию в документах на основе регулярных выражений, ключевых слов и свойств документов.

Централизованное управление контентом. Контентно-зависимые правила и действия создаются на основе контентных групп, позволяющих централизованно задавать типы контента, которые требуют контроля.

Возможность перекрывать права доступа. Позволяет выборочно разрешать или блокировать доступ к определенному контенту, хранимому на компьютерах в корпоративной сети, независимо от текущих прав доступа.

Проверка файлов внутри архивов. Позволяет осуществлять проверку каждого файла, содержащегося в архиве. Используется следующий алгоритм проверки: когда обнаруживается архивный файл, все файлы извлекаются из архива и анализируются по отдельности с целью обнаружения контента, для которого заданы контентно-зависимые правила и действия. Если содержимое по крайней мере одного файла, содержащегося в архиве, соответствует условиям заданных правил и действий, Cyber Protego Discovery применит ко всему архиву соответствующее правило или действие.

Все вложенные архивы также распаковываются и анализируются один за другим. Архивные файлы идентифицируются только по содержимому, а не по расширению. Поддерживаются следующие форматы архивов: 7z (.7z), ZIP (.zip), GZIP (.gz, .gzip, .tgz), BZIP2 (.bz2, .bzip2, .tbz2, .tbz), TAR (.tar),

RAR (.rar), CAB (.cab), ARJ (.arj), Z (.z, .taz), CPIO (.cpio), RPM (.rpm), DEB (.deb), LZH (.lzh, .lha), CHM (.chm, .chw, .hxs), ISO (.iso), UDF (.iso), COMPOUND (.msi), WIM (.wim, .swm), DMG (.dmg), XAR (.xar), HFS (.hfs), NSIS (.exe), XZ (.xz) , MsLZ (.mslz), VHD (.vhd), FLV (.flv), SWF (.swf), а также CramFS, SquashFS (.squashfs), NTFS, FAT и MBR образы файловых систем и дисков. Разделенные на несколько частей (многотомные) архивы и защищенные паролем архивы не распаковываются.

Оптическое распознавание символов (OCR). Использование OCR-технологии позволяет распознавать и извлекать текст из отсканированных документов, сфотографированных (под углом 90 градусов к фотографируемой поверхности) документов, а также скриншотов документов, и проверять его контентно-зависимыми правилами.

OCR имеет следующие возможности:

- Целое изображение или некоторые его фрагменты могут быть перевернуты, повернуты или представлены в зеркальном виде.
- Поддерживаются малоконтрастные и неяркие изображения.
- Большинство шрифтов распознается с высокой степенью точности.

OCR имеет следующие ограничения:

- Распознавание рукописного текста или любых рукописных шрифтов не поддерживается.
- Эмбоссированные и выгравированные тексты не распознаются.
- Наилучший результат распознавания достигается на изображениях с текстом черного цвета на белом фоне.

Встроенный модуль OCR поддерживает следующие языки: арабский, болгарский, каталонский, китайский - традиционный, китайский - упрощенный, корейский, хорватский, чешский, датский, голландский, английский, эстонский, финский, французский, немецкий, венгерский, индонезийский, итальянский, латышский, литовский, норвежский, польский, португальский, румынский, русский, словацкий, словенский, испанский, шведский, турецкий и японский. Поддерживаются следующие типы файлов: BMP, Dr. Halo CUT, DDS, EXR, Raw Fax G3, GIF, HDR, ICO, IFF (за исключением Maya IFF), JBIG, JNG, JPEG/JIF, JPEG-2000, JPEG-2000 codestream, KOALA, Kodak PhotoCD, MNG, PCX, PBM/PGM/PPM, PFM, PNG, Macintosh PICT, Photoshop PSD, RAW camera, Sun RAS, SGI, TARGA, TIFF, WBMP, XBM, XPM.

Примечание
Функциональность OCR поддерживается только для клиентских компьютеров под управлением Windows 7 или более поздних версий ОС.

Обнаружение текста на изображении. Технология обнаружения текста на изображении делит графические файлы на две группы: изображения с текстом (например, отсканированные документы или скриншоты документов) и изображения без текста. В некоторых случаях технология обнаружения текста на изображении позволяет выявить ценную информацию внутри изображений, и тем самым предотвратить утечку важной информации внутри графических файлов. Поддерживаются следующие типы файлов: BMP, Dr. Halo CUT, DDS, EXR, Raw Fax G3, GIF, HDR, ICO, IFF (за исключением Maya IFF), JBIG, JNG, JPEG/JIF, JPEG-2000, JPEG-2000

codestream, KOALA, Kodak PhotoCD, MNG, PCX, PBM/PGM/PPM, PFM, PNG, Macintosh PICT, Photoshop PSD, RAW camera, Sun RAS, SGI, TARGA, TIFF, WBMP, XBM, XPM.

Проверка изображений, встроенных в документы. Позволяет осуществлять проверку каждого изображения, встроенного в файлы сохраненных писем (EML), Adobe Portable Document Format (включая зашифрованные файлы, если шифрование файла выполнено одним из следующих алгоритмов: 40-bit RC4, 128-bit RC4, 128-bit AES и 256-bit AES, и при этом разрешения, установленные на файл, не запрещают извлечение текста) (PDF), Rich Text Format (RTF), документы AutoCAD (.dwg, .dxf) и документы Microsoft Office (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx). Все встроенные изображения извлекаются из таких документов в папку Temp пользователя System и анализируются независимо от текста. Текст документов проверяется контентно-зависимыми правилами и действиями, созданными на основе следующих контентных групп: “Ключевые слова”, “Шаблоны” и “Составное”. Встроенные изображения проверяются контентно-зависимыми правилами и действиями, созданными на основе следующих контентных групп: “Ключевые слова”, “Шаблоны”, “Определение типа файла”, “Свойства документа” и “Составное”. Соответствующее действие будет применено к документу в целом, если либо текст, либо любое из изображений, встроенных в документ, соответствуют какому-либо из заданных Правил и действий.

Примечание
Анализ изображений, встроенных в документы AutoCAD (.dwg, .dxf), поддерживается исключительно для клиентских компьютеров под управлением Windows XP или более поздних версий ОС.

Как работает Cyber Protego Discovery

Cyber Protego Discovery может сканировать удаленные компьютеры, применяя один из трех методов, описанных ниже.

1. Cyber Protego Discovery может осуществлять сканирование удаленных компьютеров по протоколу SMB.
2. Альтернативным методом является сканирование посредством собственных легких агентов Cyber Protego Discovery.
3. Наконец, Cyber Protego Discovery может сканировать удаленные компьютеры, используя легкий агент Discovery, встроенный в Cyber Protego Agent.

В зависимости от частных конфигураций сетевой инфраструктуры и системных требований администраторы могут выбирать те или иные методы сканирования.

Метод сканирования по протоколу SMB является наиболее простым. Он не требует ни установки программного обеспечения Cyber Protego, ни какой-либо дополнительной настройки в локальных целевых точках сканирования. Это идеальный метод для удаленного фонового сканирования общих сетевых ресурсов на устройствах NAS, а также на файловых серверах и других компьютерах, работающих под управлением любых операционных систем, включая те, на которых Cyber Protego не может быть установлен.

Использование **Cyber Protego Agent Discovery** является оптимальным для сканирования удаленных компьютеров, на которых не установлен Cyber Protego Agent. Данный метод требует развертывания агентов Discovery на всех компьютерах, где должно быть проведено сканирование.

Применение **Cyber Protego Agent** в целях сканирования - это наилучшее решение для тех, кто уже использует Cyber Protego. Поскольку данный метод использует уже установленный Cyber Protego Agent, дополнительное развертывание не требуется. Обратите внимание, что данным способом возможно сканирование исключительно компьютеров под управлением Windows, на которых уже установлен Cyber Protego Agent, но невозможно сканирование компьютеров Mac, а также компьютеров и сетевых устройств с неподдерживаемыми операционными системами (например, сканирование NAS-устройств).

Cyber Protego Discovery предполагает настройку для выполнения определенных действий с файлами, которые обнаружены в результате сканирования. Так, может быть задано удаление или зашифровывание определенных файлов, изменение прав доступа к файлам, отправка тревожного алерта администратору, запись события в журнал или уведомление пользователя сканируемого компьютера.

Результаты сканирования и журналы хранятся в централизованной базе данных SQL-сервера. Создаваемые HTML-отчеты хранятся в той же базе данных. Анализируя отчеты, администраторы могут получить точное представление о результатах сканирования, а также просмотреть список файлов, обнаруженных Cyber Protego Discovery. Отчет создается каждый раз по завершению задачи сканирования.

Обнаружение документов в Elasticsearch

Cyber Protego Discovery позволяет эффективно обнаруживать интересующие документы в Elasticsearch - распределенной программной системе, обеспечивающей индексирование и поиск различных типов данных в реальном времени. Сервер Discovery запрашивает поиск документов по заданным параметрам, а затем применяет правила и действия обнаружения к полученным от Elastcicsearch документам.

Установка Cyber Protego Agent Discovery на узел Elasticsearch не производится. Обнаружение выполняется путем прямого HTTP-доступа к узлам Elasticsearch. Действия при обнаружении ограничиваются протоколированием событий и отправкой алертов. Сервер Discovery не может изменять и удалять документы в Elasticsearch.

Подробнее см. в разделе Подразделения Elasticsearch.

Системные требования для агента сканирования

Cyber Protego Agent Discovery может использоваться для сканирования компьютеров, которые удовлетворяют следующим требованиям:

Операционная система	Microsoft Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.

Память (ОЗУ)	Минимум: 512 MB
Свободное место на жестком диске	Минимум: 200 MB
Процессор	Минимум: Intel Pentium 4

Cyber Protego Agent может использоваться для сканирования компьютеров, которые удовлетворяют следующим требованиям:

Операционная система для Cyber Protego Agent для Windows	Microsoft Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Память (ОЗУ)	Минимум: 512 МБ
Свободное место на жестком диске	Минимум: 400 МБ
Процессор	Минимум: Intel Pentium 4
Поддерживаемые средства виртуализации	Microsoft Remote Desktop Services (RDS), Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox и Windows Virtual PC.

Лицензирование

Cyber Protego Discovery лицензируется отдельно от Cyber Protego.

Если вы хотите пользоваться возможностями Cyber Protego Discovery, то для этого необходимо приобрести лицензии Cyber Protego Discovery. Cyber Protego Discovery лицензируется для каждого компьютера. Лицензия требуется для каждого компьютера или сетевого устройства, сканируемого Cyber Protego Discovery, независимо от того, настроена система для сканирования одной папки или всего компьютера целиком.

Для обнаружения документов в Elasticsearch требуется одна лицензия Cyber Protego Discovery на каждый индекс Elasticsearch, по которому будет производиться поиск документов. Число поисковых индексов не может превышать общего числа доступных лицензий Cyber Protego Discovery.

Пробный период для Cyber Protego Discovery составляет 30 дней. Пробной версией могут сканироваться не более двух компьютеров.

Установка Cyber Protego Discovery

Для установки Cyber Protego Discovery необходимо установить Search and Discovery Server (см. Установка Search and Discovery Server) и предоставить лицензию Cyber Protego Discovery (см. Установка лицензии Cyber Protego Discovery далее в этом документе).

Для управления и использования Cyber Protego Discovery необходима консоль Центральная консоль управления.

Установка Search and Discovery Server

В данном разделе описаны шаги по установке Search and Discovery Server:

1. Подготовка к установке
2. Запуск установки
3. Настройка и завершение установки

Подготовка к установке

Прежде чем приступать к установке, примите во внимание следующее:

- Программа установки Search and Discovery Server устанавливает два компонента Cyber Protego: Сервер поиска и Сервер Discovery.
- Для установки и работы Search and Discovery Server должны быть выполнены следующие требования к системе:

Операционная система	Microsoft Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Сервер базы данных	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 или 2019, любой выпуск, в том числе SQL Server Express. **Внимание** Сервер базы данных необходим для работы Сервера поиска и сервера Discovery (см. Настройка базы данных).
Свободное место на жестком диске	Минимум: 1 ГБ Рекомендуется: 800 ГБ (в случае локального сервера базы данных)

- Для установки Search and Discovery Server требуются права локального администратора.
- В целях наилучшей производительности и надежности рекомендуется устанавливать Cyber Protego Management Servers и Search and Discovery Server на разных компьютерах.
- Для Сервера поиска необходимо приобрести специальную лицензию. Одну и ту же лицензию можно установить на любом количестве компьютеров, на которых работает Search and

Discovery Server.

Лицензирование Сервера поиска основано на количестве записей в журналах, которые будут индексироваться для полнотекстового поиска. Каждая лицензия позволяет индексировать 1 000 записей в журнале теневого копирования (включая теневые копии документов), 1 000 записей в журнале активности пользователей (включая записи ввода с клавиатуры) и по 5 000 записей в каждом из прочих журналов (журнал аудита, журнал удаленных данных теневого копирования, журнал сервера, журнал мониторинга и журнал политик).

Требуемое количество лицензий Сервера поиска зависит от количества записей в журналах Cyber Protego Management Server. Максимально возможное количество индексируемых записей вычисляется исходя из общего числа установленных лицензий. При необходимости можно в любое время приобрести и установить дополнительные лицензии.

Пробный период для Search and Discovery Server составляет 30 дней. В течение этого периода сервер может индексировать 2 000 записей в журнале теневого копирования, 2 000 записей в журнале активности пользователей и по 10 000 записей в каждом из прочих журналов.

- Для сервера Discovery необходимо приобрести специальную лицензию на Cyber Protego Discovery. Лицензия требуется для каждого компьютера или сетевого ресурса, который требуется сканировать с помощью Cyber Protego Discovery, независимо от того, сканируется весь компьютер или только отдельная папка. Период пробной эксплуатации Cyber Protego Discovery составляет 30 дней. В течение этого периода можно сканировать не более двух компьютеров или сетевых ресурсов.
- Если в сети имеется несколько экземпляров Cyber Protego Management Server, то для распределения нагрузки можно также установить несколько экземпляров Search and Discovery Server.
- Если установлено несколько экземпляров Search and Discovery Server, каждый из них будет использовать собственный индекс для поиска. Следовательно, чтобы получить полный набор результатов поиска по всем данным, хранящимся на всех экземплярах Cyber Protego Management Server, понадобится выполнить одинаковые поисковые запросы на каждом экземпляре Search and Discovery Server.
- Предусмотрены два варианта сопряжения Search and Discovery Server и сервера базы банных. Перед установкой Search and Discovery Server выберите подходящий для вас вариант:
  1. ОДИН К ОДНОМУ - Устанавливается один сервер Search and Discovery Server с подключением к одному серверу базы данных. Этот вариант подходит для небольших сетей (до нескольких сотен компьютеров).
  2. МНОГИЕ КО МНОГИМ - Устанавливаются нескольких серверов Search and Discovery Server с подключением каждого к индивидуальному серверу базы данных. Этот вариант подходит для средних и крупных сетей, географически разделенных на несколько сегментов.
- Перед запуском программы установки следует закрыть все приложения, ранее запущенные в Windows.

Запуск установки

Используйте следующую процедуру для начала процесса установки.

Чтобы начать установку

1. Откройте архив DLP.zip, а затем дважды щелкните файл setup_sds.exe, чтобы запустить программу установки.
   Программу установки нужно запускать на каждом компьютере, где требуется установить Search and Discovery Server.
2. Следуйте инструкциям в программе установки.
3. На странице **Лицензионное соглашение** ознакомьтесь с лицензионным соглашением и нажмите кнопку **Я принимаю условия лицензионного соглашения**, чтобы принять условия лицензионного соглашения и продолжить установку.
4. На странице **Сведения о пользователе** введите свое имя и название организации и нажмите кнопку **Далее**.
5. На странице **Папка назначения** примите папку установки по умолчанию или нажмите кнопку **Изменить**, чтобы выбрать другую папку. Нажмите кнопку **Далее**.
   Папка установки по умолчанию - %ProgramFiles%\DeviceLock Content Security Server на 32-битной Windows или %ProgramFiles(x86)%\DeviceLock Content Security Server на 64-битной.
6. На странице **Система готова к установке программы** нажмите кнопку **Установить**, чтобы начать установку.
   Появится мастер настройки Search and Discovery Server.

   Если вы устанавливаете обновление Search and Discovery Server или переустанавливаете его и не хотите ничего менять в текущих настройках, нажмите кнопку **Далее**, и затем нажмите кнопку **Отмена**, чтобы закрыть мастер настройки.

   Если требуется изменить какие-либо параметры, сохраняя все остальные настройки, измените только необходимые параметры, пройдите через все страницы мастера настройки и нажмите кнопку **Готово** на последней странице.

   Примечание
   Если вы устанавливаете Search and Discovery Server в первый раз на данный компьютер и при этом закрываете мастер настройки, не задав параметры запуска службы Search and Discovery Server, программа установки не сможет настроить эту службу, и будет снова предложено использовать мастер настройки.

Настройка и завершение установки

Мастер настройки запускается автоматически в процессе установки и предоставляет следующие страницы для настройки Search and Discovery Server:

- Учетная запись службы и параметры подключения
- Администраторы сервера и сертификат
- Информация о лицензии
- Настройка базы данных
- Завершение настройки

Учетная запись службы и параметры подключения

На первой странице мастера настройки задается учетная запись запуска службы Search and Discovery Server и выбирается TCP-порт для подключения к этому серверу.

Входить в систему как

Необходимо задать учетную запись для запуска службы Search and Discovery Server. Это может быть локальная учетная запись системы или другая учетная запись.

Для запуска службы под учетной записью системы, выберите опцию **Локальная учетная запись системы**. Следует помнить, что программы, работающие под этой учетной записью, не могут получить доступ к сетевым ресурсам и авторизуются на удаленных компьютерах как анонимный непривилегированный пользователь. Таким образом, Search and Discovery Server, запущенный под локальной учетной записью системы, не сможет получить доступ к сетевым ресурсам, и должен будет использовать сертификат Cyber Protego для авторизации на сервере Cyber Protego Management Server, работающем на удаленном компьютере.

Дополнительную информацию о методах авторизации можно найти в описании параметра Имя сертификата.

Внимание
Если служба Search and Discovery Server запускается под учетной записью системы, то Сервер Discovery не сможет устанавливать и удалять агенты Discovery на удаленных компьютерах.

Для запуска службы под другой учетной записью выберите опцию **Данная учетная запись** и введите имя пользователя и его пароль. Рекомендуется использовать учетную запись пользователя с правами администратора на всех компьютерах, где работает Cyber Protego Management Server. В противном случае для авторизации потребуется использовать сертификат Cyber Protego.

При установке Search and Discovery Server в домене Active Directory для запуска службы рекомендуется использовать учетную запись, включенную в группу администраторов домена (Domain Admins). В результате агент получит права администратора на всех компьютерах данного домена, поскольку группа администраторов домена по умолчанию входит в локальную группу администраторов на каждом компьютере, подключенном к домену.

Необходимо также учитывать следующие соображения:

- Если на удаленном сервере Cyber Protego Management Server не используется режим безопасности по умолчанию (снят флажок **Включить безопасность по умолчанию**), то на таком сервере учетная запись, указанная в параметре **Данная учетная запись**, должна быть в списке администраторов с уровнем доступа как минимум **Только чтение**. В противном случае для авторизации потребуется использовать сертификат Cyber Protego.
- Если на удаленном Cyber Protego Agent не используется режим безопасности по умолчанию (снят флажок **Включить безопасность по умолчанию**), то на таком агенте учетная запись, указанная в параметре **Данная учетная запись**, должна быть в списке администраторов Cyber

Protego с уровнем доступа как минимум **Только чтение**. В противном случае потребуется использовать авторизацию по сертификату Cyber Protego или задать имя и пароль альтернативной учетной записи для соответствующего подразделения Cyber Protego Discovery.

Настройки подключения

Search and Discovery Server можно настроить на использование определенного TCP-порта для связи с консолью управления: выберите опцию **Фиксированный TCP-порт** и введите номер порта. Для автоматического выбора порта выберите опцию **Динамическая привязка портов**. По умолчанию Search and Discovery Server использует порт 9134.

Нажмите кнопку **Далее**, чтобы запустить службу Search and Discovery Server и перейти на вторую страницу мастера.

Запуск службы Search and Discovery Server

Если пользователь, запустивший мастер настройки, не является администратором Search and Discovery Server (в ситуации, когда устанавливается обновление поверх уже настроенного сервера), мастер настройки не сможет установить службу сервера и внести изменения в его параметры. Появится следующее сообщение: “Доступ запрещен.” Та же ошибка может возникнуть, если этот пользователь не обладает правами администратора на компьютере, где выполняется установка Search and Discovery Server.

Если для параметра **Данная учетная запись** указано несуществующее имя пользователя или неправильно введен пароль, то операционная система не сможет запустить службу Search and Discovery Server. Появится следующее сообщение: “Имя учетной записи задано неверно или не существует, или же неверен указанный пароль.”

Если учетная запись, указанная в параметре **Данная учетная запись**, не является членом группы администраторов домена (Domain Admins), появится следующее сообщение: “Учетная запись <имя> не принадлежит к группе администраторов домена. Вы хотите продолжить?”

Можно продолжить, нажав кнопку **Да**. При этом должны быть выполнены перечисленные ниже требования.

Для Сервера поиска:

- Указанная учетная запись должна обладать правами администратора на всех удаленных компьютерах, на которых работает Cyber Protego Management Server.

  - или -

- Секретный ключ сертификата Cyber Protego должен быть установлен на каждом компьютере, где работает Cyber Protego Management Server.

Для сервера Discovery:

- Указанная учетная запись должна обладать правами администратора на всех компьютерах, сканируемых сервером Discovery. Это компьютеры, на которых работает Cyber Protego Agent или агент Discovery, а также компьютеры, сканирование которых будет производиться без использования агентов.

- или -

- Открытый ключ сертификата Cyber Protego должен быть установлен на каждом компьютере (с установленным Cyber Protego Agent), который подлежит сканированию сервером Discovery.

  - или -

- Данные альтернативной учетной записи (имя пользователя и пароль) должны быть заданы в настройках сканирования.

Если учетная запись, указанная для параметра **Данная учетная запись**, не обладает системной привилегией “Входить в систему как агент”, мастер настройки автоматически присвоит ей эту привилегию. Данная привилегия необходима для запуска службы под учетной записью пользователя. Появится следующее сообщение: “Для учетной записи <имя> добавлено право входить в систему как агент.”

Если параметры запуска заданы верно, выполняется запуск службы. Появляется следующее сообщение: “Пожалуйста, подождите, пока программа взаимодействует со службой. Запуск службы DLCSS на компьютере: Локальный компьютер…”

Запуск службы Search and Discovery Server занимает некоторое время (около минуты), после чего отображается вторая страница мастера настройки.

Администраторы сервера и сертификат

На этой странице мастера можно задать список пользователей, имеющих административные права доступа к Cyber Protego Search and Discovery Server, а также установить закрытый ключ сертификата Cyber Protego (при необходимости).

Включить безопасность по умолчанию

При контроле доступа к Cyber Protego Management Server по умолчанию любые пользователи, обладающие правами локального администратора, могут подключаться к Cyber Protego Search and Discovery Server с помощью консоли управления, изменять его настройки, выполнять поисковые запросы, настраивать параметры обнаружения контента и запускать задачи обнаружения.

Чтобы включить контроль доступа по умолчанию, установите флажок **Включить безопасность по умолчанию**.

Если требуется более гибкий контроль доступа к Cyber Protego Search and Discovery Server, отключите контроль по умолчанию, сняв флажок **Включить безопасность по умолчанию**.

Если флажок **Включить безопасность по умолчанию** снят, нужно задать список учетных записей (пользователей и/или групп), которые смогут подключаться к Cyber Protego Search and Discovery Server. Чтобы добавить нового пользователя или группу пользователей в список учетных записей, нажмите кнопку **Добавить**. Можно добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку **Удалить**. Используя клавиши Ctrl и/или Shift, вы сможете выделить и удалить несколько записей одновременно.

Чтобы установить, какие действия разрешены пользователю или группе, выберите требуемый уровень доступа к серверу:

- **Полный доступ** позволяет устанавливать и удалять сервер Cyber Protego Search and Discovery Server, подключаться к нему с помощью консоли Cyber Protego Центральная консоль управления и выполнять любые действия на сервере, в том числе просматривать и изменять Общие настройки; создавать и запускать поисковые запросы и задачи; просматривать и изменять настройки обнаружения контента; создавать и запускать задачи и отчеты обнаружения контента.
- **Изменение** - То же, что и полный доступ к серверу, за исключением права вносить изменения в список администраторов сервера, а также права изменять уровень доступа к серверу для пользователей и групп, уже имеющихся в этом списке.
- **Только чтение** позволяет подключаться к серверу Cyber Protego Search and Discovery Server с помощью консоли Cyber Protego Центральная консоль управления, просматривать Общие настройки, выполнять поисковые запросы, просматривать и запускать уже имеющиеся поисковые задачи, просматривать настройки обнаружения контента, а также просматривать отчеты по результатам сканирования и обнаружения и вручную создавать новые отчеты на основе существующих отчетов и данных, подготовленных задачами сканирования и обнаружения контента. Не позволяет запускать такие задачи, вносить какие-либо изменения на сервере или создавать новый индекс для Сервера поиска.

Для пользователей и групп с уровнем доступа **Изменение** или **Только чтение** можно выбрать опцию **Доступ к теневым копиям**, чтобы обеспечить доступ к теневым копиям и записям активности пользователей. Пользователи и группы, для которых выбрана эта опция, могут выполнять поиск по содержимому теневых копий и записей активности пользователей, а также открывать, просматривать и сохранять теневые копии и записи активности пользователей, обнаруженные в результате поиска.

Администраторы Search and Discovery Server, у которых нет доступа к теневым копиям, не могут открывать, просматривать и сохранять теневые копии и записи активности пользователей. На результатах поиска нет ссылок **Открыть**, **Сохранить** и **Просмотр**, а вместо текстовых фрагментов теневых копий и записей активности пользователей отображаются звездочки. Логины и пароли в параметрах документа для записей активности пользователей также заменяются звездочками.

Внимание
Настоятельно рекомендуется предоставить администраторам Search and Discovery Server права локального администратора, поскольку при установке, обновлении или удалении сервера может потребоваться доступ к диспетчеру управления службами Windows (SCM) и общим сетевым ресурсам.

Имя сертификата

Чтобы использовать проверку подлинности на основе сертификата Cyber Protego, на Cyber Protego Search and Discovery Server может потребоваться установка закрытого ключа.

Предусмотрены два метода проверки подлинности Search and Discovery Server на удаленных компьютерах с работающим Cyber Protego Management Server.

- **Проверка подлинности по пользователю**. Cyber Protego Search and Discovery Server запущен под учетной записью, обладающей правами администратора Cyber Protego Management Server на удаленном компьютере. Инструкции по выбору учетной записи для запуска Cyber Protego Search and Discovery Server см. в описании параметра Входить в систему как.
- **Проверка подлинности по сертификату**. Если учетная запись, используемая для запуска службы Cyber Protego Search and Discovery Server, не обладает правами администратора Cyber Protego Management Server на удаленном компьютере, необходимо использовать проверку подлинности на основе сертификата Cyber Protego.
  Тот же закрытый ключ должен быть установлен на Cyber Protego Management Server и на Cyber Protego Search and Discovery Server.

Существует три способа проверки подлинности Cyber Protego Discovery при сканировании удаленного компьютера.

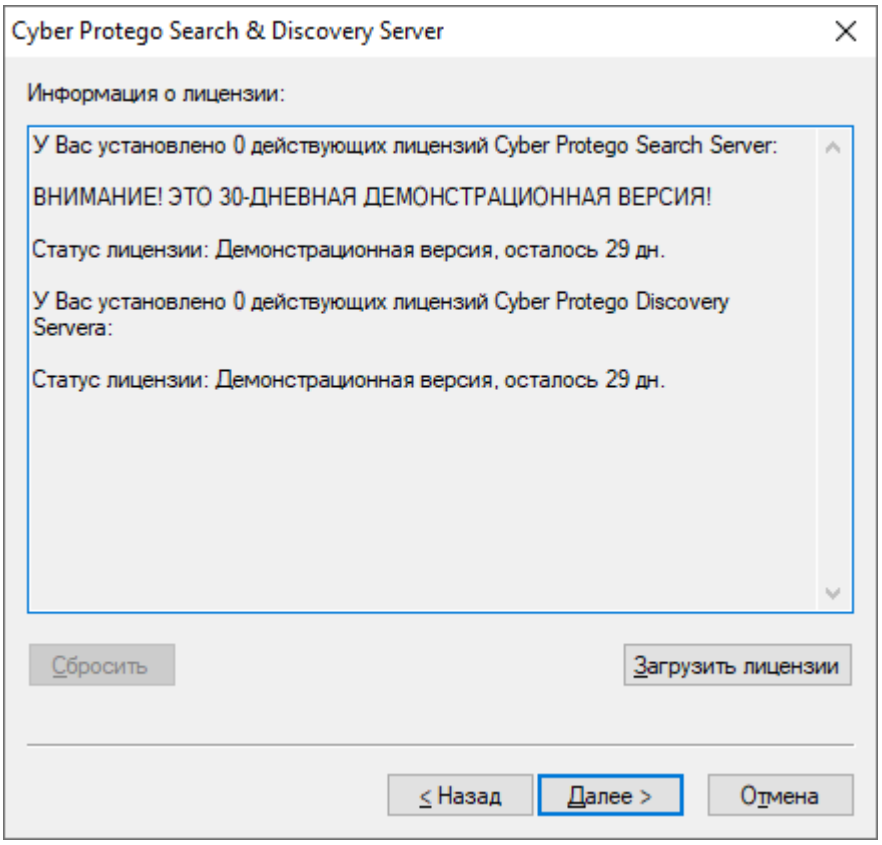
- **Проверка подлинности по пользователю**. Cyber Protego Search and Discovery Server запускается от имени учетной записи определенного пользователя, и эти учетные данные используются для доступа к удаленным компьютерам во время сканирования. Эти учетные данные могут быть предоставлены службой Cyber Protego Agent, Cyber Protego Discovery Агент или удаленным компьютером, если сканирование выполняется без агента. Подробнее о том, как запустить Cyber Protego Search and Discovery Server от имени пользователя, см. в описании параметра Входить в систему как.
- **Проверка подлинности по альтернативным учетным данным**. Cyber Protego Search and Discovery Server запускается от имени учетной записи пользователя, имеющего административные права доступа как минимум на локальном компьютере. Cyber Protego Discovery будет использовать альтернативные учетные данные для входа на удаленный компьютер перед его сканированием.
- **Проверка подлинности по сертификату Cyber Protego** выполняется на основе сертификата Cyber Protego для аутентификации на удаленных компьютерах, где запущен Cyber Protego Agent и установлен открытый ключ сертификата.

Чтобы установить сертификат Cyber Protego, нажмите кнопку ··· и выберите файл с закрытым ключом. Чтобы удалить сертификат Cyber Protego, нажмите кнопку **Удалить**.

Нажмите кнопку **Далее**, чтобы применить настройки и перейти к следующей странице мастера настройки.

Информация о лицензии

Данная страница служит для установки лицензий на Сервер поиска (Cyber Protego Search Server) и/или на Сервер Discovery (Cyber Protego Discovery). На каждый из этих серверов требуется отдельная лицензия. Период пробной эксплуатации составляет 30 дней.



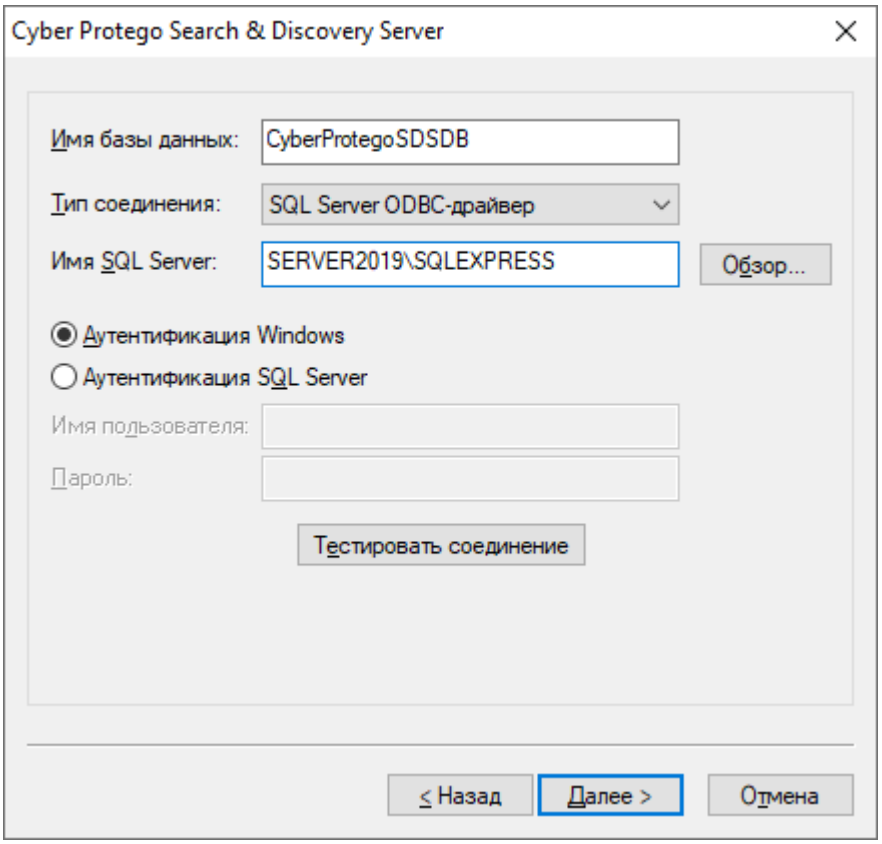
Чтобы установить лицензию, нажмите кнопку **Загрузить лицензии** и выберите файл с лицензией. Можно загрузить несколько файлов подряд - один за другим. В окне **Информация о лицензии** отображается сводная информация об устанавливаемых вами лицензиях.

После установки Search and Discovery Server можно использовать консоль Центральная консоль управления для установки лицензии или просмотра текущей информации о лицензии, включая количество установленных лицензий и количество используемых лицензий для Сервера поиска и/или сервера Discovery.

Нажмите кнопку **Далее,** чтобы перейти к настройке базы данных.

Настройка базы данных

На этой странице мастер предложит вам настроить параметры базы данных.



Внимание

Не пропускайте эту страницу, так как база данных необходима для работы функций Search and Discovery Server и Discovery. Без подключения к ней будет невозможно находить контентные группы, сохранять и автоматизировать поисковые запросы и использовать Discovery Server для обнаружения контента.

Имя базы данных

В поле **Имя базы данных** можно увидеть и изменить имя базы данных для Cyber Protego Search and Discovery Server. По умолчанию мастер рекомендует имя **CyberProtegoSDSDB**.

Примечание

Создавать базу данных с указанным именем не нужно, так как мастер настройки создает ее автоматически или использует существующую.

Тип подключения

В списке **Тип подключения** можно выбрать один из следующих вариантов:

- **Драйвер ODBC SQL Server** – подключение к Microsoft SQL Server через драйвер ODBC. Параметр **Имя сервера SQL Server** должен содержать имя компьютера, на котором работает SQL Server, а также имя экземпляра SQL Server. Имя сервера SQL Server обычно состоит из двух частей: имени компьютера и имени экземпляра, разделенных обратной косой чертой (например, компьютер\экземпляр). Если имя экземпляра пусто (экземпляр по умолчанию), то

имя компьютера используется в качестве имени сервера SQL Server. Чтобы получить имена серверов SQL Server, доступных в вашей локальной сети, нажмите кнопку **Обзор** (вам потребуется доступ к удаленному реестру компьютера SQL Server для получения имени экземпляра).

Если параметр **Имя сервера SQL Server** пуст, то это означает, что SQL Server работает на том же компьютере, что и Cyber Protego Search and Discovery Server, и имеет пустое имя экземпляра (экземпляр по умолчанию).

Для подключения к SQL Server нужно также настроить параметры проверки подлинности.

Выберите вариант **Проверка подлинности Windows**, чтобы проверка подлинности на SQL Server производилась от учетной записи, используемой для запуска службы Cyber Protego Search and Discovery Server.

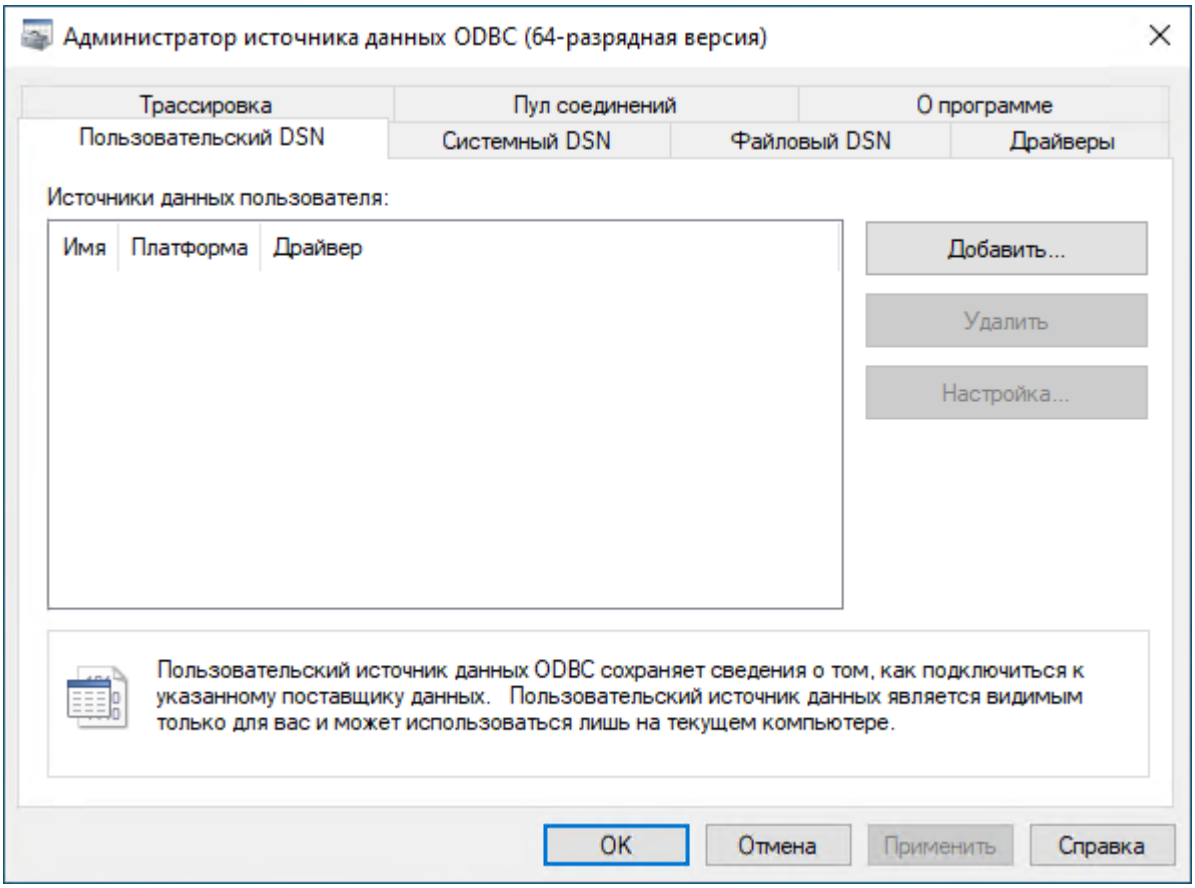
Если служба запускается от имени учетной записи SYSTEM, а SQL Server запускается на удаленном компьютере, то служба не сможет подключиться к SQL Server, так как учетная запись SYSTEM не имеет прав доступа к сети. Подробнее о том, как запустить Cyber Protego Search and Discovery Server от имени пользователя, см. в описании параметра Входить в систему как.

Выберите вариант **Проверка подлинности SQL Server**, чтобы SQL Server выполнял проверку подлинности по ранее определенным имени входа и паролю. Прежде чем выбирать вариант **Проверка подлинности SQL Server**, убедитесь, что ваш SQL Server настроен для проверки подлинности в фиксированном режиме. Введите имя пользователя SQL Server в поле **Имя входа**, а пароль в поле **Пароль**.

Примечание

Проверка подлинности Windows обеспечивает более высокий уровень защиты, чем проверка подлинности SQL Server. Используйте первый способ там, где это возможно.

- **Системный источник данных** – подключение к серверу базы данных через ранее созданный в системе источник данных. Выберите источник данных в списке **Имя источника данных**.
  Чтобы создать источник данных, воспользуйтесь оснасткой **Администратор источников данных ODBC**, выбрав **Панель управления** > **Администрирование**.



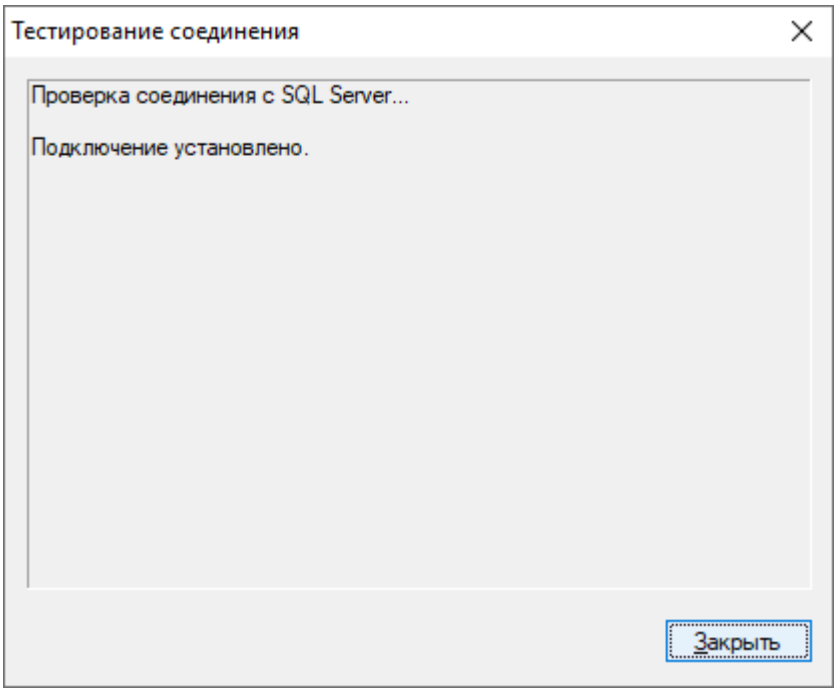
Если источнику данных требуется имя пользователя и пароль (например, при использовании проверки подлинности SQL Server), то необходимо указать их в полях **Имя входа** и **Пароль**. В противном случае оставьте эти поля пустыми.

Чтобы обновить список **Имя источника данных**, нажмите кнопку **Обновить**.

Проверка соединения

Задав параметры соединения, можно выполнить проверку, чтобы убедиться в их корректности. Для этого нажмите кнопку **Тестировать соединение**.

Проверяется только соединение с сервером базы данных. В случае успешного подключения к серверу диалоговое окно **Тестирование соединения** не покажет никаких ошибок.



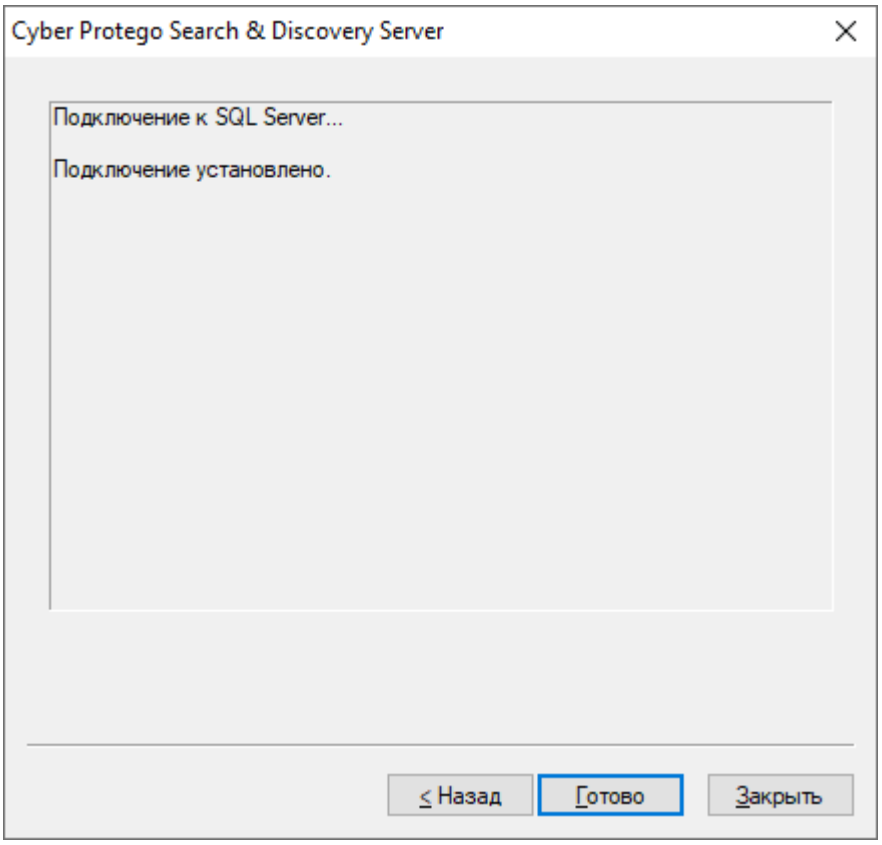
Если не удается установить соединение с использованием заданных параметров, в диалоговом окне могут появиться следующие сообщения об ошибках:

- **SQL Server does not exist or access denied** - Указано неправильное имя в параметре **Имя SQL Server**, либо компьютер, на котором работает SQL Server, недоступен. Возможно, указано имя компьютера, но не указано имя экземпляра SQL Server (имя нужно указывать в формате computer\instance).
- **Login failed for user 'COMPUTER_NAME$'** - Выбран режим аутентификации Windows, но учетная запись, под которой запущен Cyber Protego Search and Discovery Server, не может получить доступ к SQL Server. Возможно служба запущена под локальной учетной записью системы или под учетной записью, не обладающей правами администратора на компьютере SQL Server.
- **Login failed for user 'user_name'** - Выбран режим аутентификации SQL Server, но неверно задано имя пользователя SQL Server (логин) или его пароль. В параметре **Имя пользователя** должно быть указано имя пользователя SQL Server, а не пользователя Windows. Для администрирования пользователей SQL Server используются средства SQL Server (такие как Microsoft SQL Server Management Studio).
- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** - Выбран режим аутентификации SQL Server, но SQL Server не поддерживает данный режим. Необходимо либо использовать режим аутентификации Windows, либо настроить SQL Server для работы в смешанном режиме аутентификации.
- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** - Источник данных, указанный в параметре **Имя источника данных** настроен для работы в режиме аутентификации SQL Server, но параметр **Имя пользователя** не задан.
- **Data source name not found and no default driver specified** - Задано неправильное значение параметра **Имя источника данных** (например, пустая строка).

Нажмите кнопку **Далее**, чтобы применить настройки и перейти к последней странице.

Завершение настройки

Создание базы данных займет некоторое время. Если база данных уже существует на указанном сервере и имеет правильный формат (создана программой настройки Cyber Protego), то Cyber Protego Search and Discovery Server будет использовать эту существующую базу данных. При необходимости Cyber Protego автоматически обновляет базу данных до последней версии.



На данной странице мастера можно наблюдать за применением указанных параметров базы данных и просматривать ошибки, которые могут возникнуть при ее настройке.

Если не удается создать или настроить базу данных с использованием заданных параметров, в диалоговом окне могут появиться следующие сообщения об ошибках:

- **CREATE DATABASE permission denied in database 'name'** - У учетной записи, используемой для подключения к SQL Server, недостаточно прав для создания базы данных. Этой учетной записи требуется как минимум серверная роль **dbcreator** (см. **Server Roles** в Login Properties у Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context** - Учетная запись, используемая для подключения к SQL Server, не может получить доступ к существующей базе данных. Учетная запись должна быть привязана к этой базе данных (см. **User Mapping** в **Login Properties** у Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** - Учетная запись, используемая для подключения к SQL Server, не может получить доступ на чтение/запись в

существующей базе данных. Учетной записи требуются как минимум роли базы данных **db_datareader** и **db_datawriter** (см. User Mapping в Login Properties у Microsoft SQL Server Management Studio).

- **Invalid object name 'name'** - База данных, указанная в параметре **Имя базы данных**, существует на SQL Server, но имеет неверный формат. Такая ошибка обычно возникает при попытке использовать базу данных, которая повреждена или создана программой, отличной от программы настройки Cyber Protego Search and Discovery Server.
- **Cyber Protego Database has an unsupported format** - База данных, указанная в параметре **Имя базы данных**, существует на SQL Server, но имеет устаревший формат и не может быть обновлена до новой версии. Ее формат не удается преобразовать для использования совместно с новой версией Cyber Protego. Укажите имя другой базы данных или задайте новое имя, чтобы создать новую базу данных.
- **Cyber Protego Database has a format that is not supported by the current server version** - База данных, указанная в параметре **Имя базы данных**, существует на SQL Server, но она была создана новой версией Cyber Protego Search and Discovery Server. Используйте новую версию Cyber Protego Search and Discovery Server или задайте другое имя базы данных.

Помимо перечисленных выше ошибок могут появиться также некоторые ошибки, приведенные в разделе Проверка соединения ранее в этом документе.

При появлении ошибок нажмите кнопку **Назад**, чтобы вернуться на предыдущую страницу и внести необходимые изменения в настройки.

При отсутствии ошибок нажмите кнопку **Готово**, чтобы закрыть мастер настройки и продолжить процесс установки.

Далее, на странице **Мастер установки завершен** нажмите кнопку **Готово**, чтобы завершить процесс установки. С этой страницы можно перейти на веб-сайт Cyber Protego. Этот вариант выбран по умолчанию.

Примечание
Удалить Cyber Protego Search and Discovery Server можно следующим образом:

- Используйте средство **Программы и компоненты** панели управления Windows (**Установка и удаление программ** на ранних версиях Windows).
  - или -
- Выберите пункт **Удалить Cyber Protego Search and Discovery Server** в меню **Пуск** Windows.

Настройка сервера Discovery

Навигация по серверу Discovery

Прежде чем изучать функциональность сервера Cyber Protego Discovery, необходимо ознакомиться с базовой навигацией по продукту. Используйте узел **Search and Discovery Server** в консоли Cyber Protego Центральная консоль управления для настройки и использования Cyber Protego Search and Discovery Server.

Щелкните правой кнопкой мыши узел **Search and Discovery Server**, чтобы отобразить следующие команды:

- **Подключиться** – подключается к компьютеру, на котором работает сервер Cyber Protego Discovery.
  При подключении к компьютеру, на котором установлена устаревшая версия Cyber Protego Discovery, может отображаться следующее сообщение: «Версии продукта на машинах клиента и сервера не совпадают». В таком случае необходимо установить новую версию Cyber Protego Discovery на этот компьютер. Указания по установке см. в разделе Установка Cyber Protego Discovery.
- **Переподключиться** - Повторно подключается к тому же компьютеру.
- **Подключаться к последнему использованному серверу при запуске** – установите флажок рядом с этой командой, чтобы при каждом запуске консоль Cyber Protego Центральная консоль управления автоматически подключалась к серверу, который использовался в предыдущем подключении.
- **Мастер создания сертификата** – запускает программу создания сертификатов Cyber Protego.
- **Мастер создания подписи** – запускает программу для предоставления пользователям временного доступа к устройствам, а также для подписывания файлов с настройками Cyber Protego Agent.
- **О программе Cyber Protego** – отображает диалоговое окно с информацией о версии Cyber Protego и установленных лицензиях.

Разверните узел **Search and Discovery Server**, а затем выберите узел **Общие настройки**.

Этот узел можно использовать для настройки следующих общих параметров Сервера поиска и сервера Discovery.

- **Администраторы сервера** – используйте этот параметр для указания администраторов сервера и связанных с ними прав доступа.
- **Настройки Сервера поиска** – используйте этот элемент для настройки параметров, относящихся к полнотекстовому поиску.
- **Настройки Сервера Discovery** – используйте этот элемент для настройки параметров, относящихся к обнаружению контента.
- **Алерты** – используйте этот элемент для настройки параметров доставки алертов (уведомлений).

- **Сертификат Cyber Protego** – используйте этот параметр для установки, изменения или удаления пары сертификатов Cyber Protego.
- **Учетная запись сервиса при загрузке** – используйте этот параметр для указания данных стартовой учетной записи для запуска службы сервера, таких как имя и пароль учетной записи.
- **TCP-порт** – используйте этот параметр для указания TCP-порта, который консоль Cyber Protego Центральная консоль управления использует для подключения к серверу.
- **Тип соединения** – используйте этот параметр для выбора драйвера ODBC или системного источника данных для доступа к базе данных Search and Discovery Server.
- **Имя сервера SQL** – используйте этот параметр для указания сервера базы данных Cyber Protego Search and Discovery Server. Этот параметр отображается при выборе типа соединения «драйвер ODBC».
- **Системный источник данных** – используйте этот параметр, чтобы указать источник данных, через который осуществляется доступ к серверу базы данных Cyber Protego Search and Discovery Server. Этот параметр отображается при выборе типа соединения «системный источник данных».
- **Имя базы данных** – используйте этот параметр для указания имени базы данных Search and Discovery Server.
- **Имя пользователя SQL** – используйте этот параметр, чтобы указать имя входа и пароль для доступа к базе данных Cyber Protego Search and Discovery Server. Этот параметр отображается, если выбран режим «Проверка подлинности SQL Server».

Раскройте узел **Общие настройки** и выберите узел **Настройки Сервера Discovery**. С помощью этого узла можно настраивать следующие параметры, относящиеся исключительно к серверу Cyber Protego Discovery:

- **Management Server(s)** – используйте этот параметр, чтобы указать один или несколько серверов Cyber Protego Management Server, на которых размещается база данных цифровых отпечатков.
- **Лицензии Cyber Protego Discovery Server** – используйте этот параметр, чтобы установить необходимое количество лицензий Cyber Protego Discovery.
- **Параметры логирования** – используйте этот параметр, чтобы задать настройки ведения журнала для Discovery Server. Он позволяет определить типы событий, которые должны регистрироваться в журнале.
- **E-mail сообщение для алертов** – используйте этот параметр, чтобы настроить шаблон сообщений электронной почты, используемых для предупреждения администраторов о выявленном контенте.
- **Syslog-сообщение для алертов** – используйте этот параметр, чтобы настроить шаблон сообщений syslog для алертов (предупреждений).
- **Сообщение оповещения об обнаружении** – используйте этот параметр, чтобы настроить шаблон сообщения в области уведомлений на панели задач, отображаемого пользователям, которые выполнили вход в систему, когда происходит событие обнаружения.
- **Интервал сбора данных** – используйте этот параметр, чтобы указать временной промежуток между сбором данных с агентов обнаружения.

- **Проверка содержимого бинарных файлов** – используйте этот параметр для включения обнаружения контента по совпадению с ключевыми словами и по шаблонам в тексте, который содержится в произвольных двоичных файлах.

Общие настройки

Существует три типа настроек конфигурации для Cyber Protego Search and Discovery Server.

- **Общие настройки** определяют работу Cyber Protego Search and Discovery Server в целом. В текущем разделе приведены инструкции по управлению этими настройками.
- **Настройки сервера поиска** определяют работу Сервера поиска – составной части Cyber Protego Search and Discovery Server. Подробнее см. в разделе «Управление настройками Search and Discovery Server».
- **Настройки сервера Discovery** определяют работу Discovery Server. Инструкции по управлению этими настройками см. в разделе Настройки Сервера Discovery.

Администратор может настроить общие параметры сервера при установке Cyber Protego Search and Discovery Server или воспользоваться консолью Cyber Protego Центральная консоль управления для их настройки и/или изменения после того, как сервер будет установлен и запущен.

Примечание

- Управлять сервером Cyber Protego Search and Discovery Server и использовать его могут лишь администраторы сервера с достаточными правами.
- Для начала работы подключитесь из консоли Cyber Protego Центральная консоль управления к компьютеру, на котором работает Cyber Protego Search and Discovery Server: щелкните правой кнопкой мыши по узлу **Search and Discovery Server**, затем нажмите **Подключиться**. .

Из консоли Cyber Protego Центральная консоль управления администратор может выполнять следующие задачи конфигурации сервера:

- Настройка пользователей, которым разрешен доступ к Cyber Protego Search and Discovery Server.
- Изменение данных стартовой учетной записи, таких как имя или пароль учетной записи, для службы Cyber Protego Search and Discovery Server.
- Установка или удаление сертификата Cyber Protego для аутентификации обмена данными между Cyber Protego Search and Discovery Server и Cyber Protego Management Server.
- Изменение порта TCP, используемого для подключения из консоли Cyber Protego Центральная консоль управления к серверу Cyber Protego Search and Discovery Server.
- Просмотр или изменение параметров подключения Search and Discovery Server к базе данных.

Эти задачи можно выполнять как по отдельности, так и в сочетании.

Чтобы выполнить эти задачи в сочетании, воспользуйтесь мастером настройки Cyber Protego Search and Discovery Server. Этот мастер запускается автоматически при установке или обновлении Search and Discovery Server.

Чтобы выполнить комплексную настройку конфигурации

1. В дереве консоли раскройте узел **Search and Discovery Server**.
2. В узле **Search and Discovery Server** щелкните правой кнопкой мыши **Общие настройки** и выберите пункт **Свойства**.
   Откроется первая страница мастера.
3. Пройдите по страницам мастера. После завершения работы со страницей переходите к следующей, нажимая кнопку **Далее**, или возвращайтесь на предыдущую, нажимая кнопку **Назад**. На последней странице нажмите кнопку **Готово**, чтобы завершить работу мастера. Описания страниц мастера см. в разделе Выполнение настройки и завершение установки инструкции по установке Cyber Protego Search and Discovery Server.

С помощью консоли Cyber Protego Центральная консоль управления администратор может выполнять следующие задачи по настройке отдельных параметров сервера:

- Настройка доступа к Cyber Protego Search and Discovery Server
- Настройка учетной записи для запуска службы
- Установка или удаление сертификата Cyber Protego
- Настройка TCP-порта
- Управление параметрами подключения к базе данных

Настройка доступа к Search and Discovery Server

Предусмотрена возможность указать, кому именно разрешено работать с сервером Search and Discovery Server. Это позволяет защитить сервер от несанкционированного доступа и внешних атак.

Чтобы указать, какие пользователи могут иметь доступ к серверу

1. В дереве консоли раскройте узел **Search and Discovery Server**.
2. В узле **Search and Discovery Server** выполните одно из следующих действий:
   - Выберите **Общие настройки**. На панели сведений дважды щелкните **Администраторы сервера** или щелкните правой кнопкой мыши **Администраторы сервера** и затем выберите команду **Свойства**.

     - или -
   - Раскройте узел **Общие настройки**. В узле **Общие настройки** щелкните правой кнопкой мыши **Администраторы сервера**, а затем выберите команду **Свойства**.
3. В появившемся диалоговом окне **Search and Discovery Server** выполните следующие действия:
   Чтобы включить защиту по умолчанию
   - Установите флажок **Включить безопасность по умолчанию**.

   Если включена защита по умолчанию, члены локальной группы Администраторы получат полный доступ к Search and Discovery Server.

   Чтобы предоставить доступ к серверу отдельным пользователям

a. Снимите флажок **Включить безопасность по умолчанию**.

b. Под областью **Пользователи** нажмите кнопку **Добавить**, чтобы добавить пользователей, которым необходимо предоставить доступ к серверу Search and Discovery Server.

c. В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

   Выбранные пользователи/группы становятся администраторами сервера и отображаются в области **Пользователи** диалогового окна **Search and Discovery Server**. Администраторы сервера имеют право выполнять задачи, связанные с настройкой и использованием Search and Discovery Server, и по умолчанию они имеют полный доступ к серверу.

   Чтобы изменить уровень доступа к серверу для какого-либо администратора, выберите соответствующего пользователя или группу в области **Пользователи**, а затем в списке прав доступа выберите один из следующих вариантов:

- **Полный доступ** - Позволяет устанавливать и удалять сервер Search and Discovery Server, подключаться к нему с помощью Центральной консоли управления и выполнять любые действия на сервере, в том числе: просматривать и изменять Общие настройки; создавать и запускать поисковые запросы и задачи; просматривать и изменять настройки обнаружения контента; создавать и запускать задачи и отчеты обнаружения контента.
- **Изменение** - То же, что и полный доступ к серверу, за исключением права вносить изменения в список администраторов сервера, а также права изменять уровень доступа к серверу для пользователей и групп, уже имеющихся в этом списке.
- **Только чтение** - Позволяет подключаться к серверу Search and Discovery Server с помощью Центральной консоли управления, просматривать Общие настройки, выполнять поисковые запросы, просматривать и запускать уже имеющиеся поисковые задачи, просматривать настройки обнаружения контента, а также просматривать отчеты по результатам сканирования и обнаружения и вручную создавать новые отчеты на основе существующих отчетов и данных, подготовленных задачами сканирования и обнаружения контента. Не позволяет запускать такие задачи, вносить какие-либо изменения на сервере, или создавать новый индекс для Сервера поиска.

Для пользователей и групп с уровнем доступа **Изменение** или **Только чтение** можно выбрать опцию **Доступ к теневым копиям**, чтобы обеспечить доступ к теневым копиям и записям активности пользователей. Пользователи и группы, для которых выбрана эта опция, могут выполнять поиск по содержимому теневых копий и записей активности пользователей, а также открывать, просматривать и сохранять теневые копии и записи активности пользователей, обнаруженные в результате поиска.

Администраторы Search and Discovery Server, у которых нет доступа к теневым копиям, не могут открывать, просматривать и сохранять теневые копии и записи активности пользователей. На результатах поиска нет ссылок **Открыть**, **Сохранить** и **Просмотр**, а вместо текстовых фрагментов теневых копий и записей активности пользователей отображаются звездочки. Логины и пароли в параметрах документа для записей активности пользователей также заменяются звездочками.

Примечание
Настоятельно рекомендуется, чтобы администраторам Search and Discovery Server были предоставлены права локального администратора.

Чтобы отозвать права администратора сервера у какого-либо пользователя или группы, выберите этого пользователя или группу в области **Пользователи**, а затем нажмите кнопку **Удалить**.

Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

4. Нажмите кнопку **OK**.

Настройка стартовой учетной записи службы сервера

Спустя какое-то время может понадобиться изменить стартовую учетную запись службы Search and Discovery Server, выбранную в процессе установки. Также может потребоваться изменить пароль этой учетной записи.

Чтобы изменить имя или пароль стартовой учетной записи службы сервера

1. В дереве консоли раскройте узел **Search and Discovery Server**.
2. В узле **Search and Discovery Server** выберите **Общие настройки**.
3. На панели сведений дважды щелкните **Учетная запись сервиса при загрузке** или щелкните правой кнопкой мыши **Учетная запись сервиса при загрузке** и затем выберите команду **Свойства**.
4. В появившемся диалоговом окне **Search and Discovery Server** выполните следующие действия:

   Чтобы изменить стартовую учетную запись службы сервера

   a. В области **Входить в систему как** нажмите кнопку **Обзор**.

   b. В появившемся диалоговом окне **Выбор: "Пользователь"** в поле **Введите имена выбираемых объектов** введите имя пользователя, и затем нажмите кнопку **OK**.
   Выбранный пользователь отображается в поле **Данная учетная запись** диалогового окна **Search and Discovery Server**.

   Настоятельно рекомендуется использовать учетную запись, обладающую правами администратора на всех компьютерах, где установлен Cyber Protego Management Server. В домене Active Directory рекомендуется использовать учетную запись, являющуюся членом группы “Администраторы домена”. В противном случае будет необходимо использовать авторизацию по сертификату Cyber Protego.

   Чтобы изменить пароль учетной записи службы сервера

   a. В области **Входить в систему как** введите новый пароль в поле **Пароль**.

   b. Повторно введите новый пароль в поле **Подтверждение пароля**.

   Чтобы назначить учетную запись СИСТЕМА для службы сервера

   - В области **Входить в систему как** выберите опцию **Локальная учетная запись системы**.

Примечание

Если агент сервера использует учетную запись СИСТЕМА (Local System), то Сервер Discovery:

- Не может получить доступ к агентам Discovery на удаленных компьютерах. В таком случае для авторизации должен использоваться сертификат Cyber Protego.
- Не может устанавливать и удалять агенты Discovery на удаленных компьютерах.

5. Нажмите кнопку **OK**.

Установка или удаление сертификата Cyber Protego

Сервер Discovery не получить доступ к агенту Discovery из-за недостаточных прав доступа стартовой учетной записи службы Search and Discovery Server. В этом случае необходимо настроить аутентификацию по сертификату Cyber Protego, установив его секретный ключ на сервере Search and Discovery Server. Публичный ключ сертификата должен быть установлен для Cyber Protego Agent на компьютерах, сканируемых агентом Discovery.

Чтобы установить или удалить сертификат Cyber Protego на сервере Search and Discovery Server

1. В дереве консоли раскройте узел **Search and Discovery Server**.
2. В узле **Search and Discovery Server** выберите **Общие настройки**.
3. На панели сведений дважды щелкните **Сертификат Cyber Protego** или щелкните правой кнопкой мыши **Сертификат Cyber Protego** и затем выберите команду **Свойства**.
4. В появившемся диалоговом окне **Search and Discovery Server** выполните следующие действия:

   Чтобы установить секретный ключ сертификата Cyber Protego

   a. Нажмите кнопку рядом с полем Имя сертификата, чтобы открыть диалоговое окно **Выберите файл сертификата Cyber Protego**. ...

   b. В диалоговом окне **Выберите файл сертификата Cyber Protego** выберите соответствующий файл сертификата, и нажмите кнопку **Открыть**.

   Чтобы удалить секретный ключ сертификата Cyber Protego

   - Нажмите кнопку **Удалить** рядом с полем **Имя сертификата**.
5. Нажмите кнопку **OK**.

Настройка параметра TCP-порт

Спустя какое-то время может понадобиться изменить TCP-порт для подключения Центральной консоли управления к серверу Search and Discovery Server.

Чтобы изменить TCP-порт для подключения консоли

1. В дереве консоли раскройте узел **Search and Discovery Server**.
2. В узле **Search and Discovery Server** выберите **Общие настройки**.

3. На панели сведений дважды щелкните **TCP-порт** или щелкните правой кнопкой мыши **TCP-порт** и затем выберите команду **Свойства**.
4. В области **Настройки подключения** появившегося диалогового окна **Search and Discovery Server** выполните одно из следующих действий:
   - Щелкните **Динамическая привязка портов**, чтобы использовать динамический выбор порта.

     - или -
   - Щелкните **Фиксированный TCP-порт**, чтобы использовать заданный порт. Затем введите требуемый номер порта в поле **Фиксированный TCP-порт**.
     По умолчанию Search and Discovery Server использует порт 9134.
5. Нажмите кнопку **OK**.

Настройка подключения к базе данных

Подключение к базе данных необходимо для работы и сервера Discovery. Если подключение к базе данных не настроено, недоступными оказываются все функции сканирования контента. Используя консоль, можно просмотреть или изменить параметры подключения к базе данных.

Чтобы просмотреть или изменить параметры подключения к базе данных

1. В дереве консоли раскройте узел **Search and Discovery Server**.
2. В узле **Search and Discovery Server** выберите **Общие настройки**.
3. На панели сведений дважды щелкните любой из следующих параметров: **Тип соединения**, **Имя SQL Server**, **Имя базы данных** или **Имя пользователя SQL**. Можно также щелкнуть параметр правой кнопкой мыши и затем выбрать команду **Свойства**.
4. В появившемся диалоговом окне можно просмотреть или изменить следующие параметры:
   - **Имя базы данных** - Имя базы данных Search and Discovery Server.
   - **Тип соединения** - Определяет, использовать ли драйвер ODBC или системный источник данных для соединения с сервером базы данных Search and Discovery Server.
     Дальнейшие параметры зависят от выбранного типа соединения.
   - **Имя SQL Server** - Имя сервера базы данных (если используется драйвер ODBC).
     Пустое имя означает, что сервер базы данных находится на компьютере, на котором работает Search and Discovery Server.
   - **Аутентификация Windows** / **Аутентификация SQL Server** - Режим аутентификации на SQL-сервере (для драйвера ODBC Microsoft SQL Server).
   - **Имя источника данных** - Имя системного источника данных (если используется системный источник данных).
   - **Имя пользователя**, Пароль - Логин и пароль для доступа к базе данных (при использовании режима “Аутентификация SQL Server”).
   - Нажмите кнопку **Далее** и дождитесь завершения операции. Затем нажмите кнопку **Готово**.

Подробнее о параметрах подключения к базе данных см. в разделе Настройка базы данных инструкции по установке Search and Discovery Server.

Настройки Сервера Discovery

Для настройки сервера Discovery предусмотрены следующие параметры:

- **Cyber Protego Management Server** - Позволяет указать Cyber Protego Management Servers, обслуживающие базу данных цифровых отпечатков.
- **Лицензии Discovery Server** - Позволяет установить лицензию Cyber Protego Discovery.
- **Параметры логирования** - Позволяет выбрать типы событий для записи в журнал задач Discovery.
- **E-mail сообщение для алертов** - Позволяет настроить сообщение алертов Discovery для отправки по электронной почте (SMTP).
- **Syslog-сообщение для алертов** - Позволяет настроить сообщение алертов Discovery для отправки на сервер syslog.
- **Сообщение оповещения об обнаружении** - Позволяет настроить всплывающее сообщение Discovery, отображаемое в системной области уведомлений (панели задач) сканируемого компьютера.
- **Интервал сбора данных** - Позволяет задать временной интервал, через который Агент Discovery начинает сообщать о наличии новых данных для передачи на Сервер Discovery.
- **Проверка содержимого бинарных файлов** - Позволяет обнаруживать ключевые слова и шаблоны в текстовом содержимом произвольных двоичных файлов.

Чтобы начать настройку параметра, дважды щелкните этот параметр, или щелкните его правой кнопкой мыши и используйте команды в появившемся контекстном меню.

Управление параметрами сервера Discovery предполагает следующие задачи:

- Задание серверов базы данных цифровых отпечатков
- Установка лицензии Cyber Protego Discovery
- Настройка параметров логирования
- Настройка сообщений для алертов и оповещений
- Изменение интервала сбора данных
- Включение проверки содержимого двоичных файлов

Задание серверов базы данных цифровых отпечатков

Для обнаружения контента по цифровым отпечаткам требуется указать хотя бы один Cyber Protego Management Server, на котором находится база данных отпечатков.

Чтобы указать один или несколько серверов базы данных цифровых отпечатков, щелкните правой кнопкой мыши **Cyber Protego Management Server** в разделе **Настройки сервера Discovery** и выберите **Свойства**, либо дважды щелкните **Cyber Protego Management Server** в этом разделе. Затем используйте появившееся диалоговое окно, чтобы просмотреть или изменить список серверов.

Чтобы добавить сервер в список, введите имя компьютера, на котором установлен Cyber Protego Management Server. Это может быть полное доменное имя (FQDN), короткое имя или IP-адрес компьютера. Чтобы добавить несколько серверов, введите имена компьютеров, разделенные точкой с запятой (;).

Можно изменить или удалить отдельные имена компьютеров из списка. Чтобы очистить список, нажмите кнопку **Удалить**.

Добавление лицензий Cyber Protego Discovery

Для использования технологий сканирования и обнаружения контента необходимо приобрести специальные лицензии Cyber Protego Discovery, соответственно количеству компьютеров или сетевых ресурсов, подлежащих сканированию (далее упоминаются только компьютеры).

Модель лицензирования Cyber Protego Discovery основана на совокупном числе компьютеров, которые будут сканироваться Cyber Protego Discovery. Одна лицензия позволяет сканировать один компьютер, независимо от того, будет ли сканироваться весь компьютер или отдельная папка на этом компьютере.

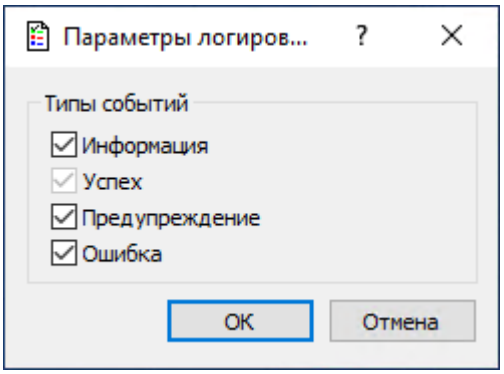
В зависимости от общего количества компьютеров в корпоративной сети, которые должны сканироваться Cyber Protego Discovery, следует приобрести соответствующее число лицензий. Если используется несколько лицензий на Cyber Protego Discovery, то количество компьютеров, подлежащих сканированию, будет суммироваться исходя из количества лицензий. Период пробной эксплуатации для Cyber Protego Discovery составляет 30 дней. В течение пробного периода можно проводить сканирование не более чем двух компьютеров. Приобрести и установить дополнительные лицензии Cyber Protego Discovery можно в любое время.

Для установки дополнительных лицензий Cyber Protego Discovery выберите узел **Настройки сервера Discovery** в дереве консоли, затем дважды щелкните **Лицензии Discovery Server** на панели сведений. В появившемся диалоговом окне нажмите кнопку **Загрузить лицензии** для выбора файла лицензии. Можно загрузить несколько файлов подряд - один за другим.

После успешной загрузки файла с лицензией в диалоговом окне можно просмотреть сводку информации о лицензии, в которой поле **Всего лицензий** отображает общее количество установленных лицензий, а поле **Использовано лицензий** отображает количество лицензий, используемых в настоящее время для сканирования компьютеров или сетевых устройств с помощью Cyber Protego Discovery.

Настройка параметров логирования

Дважды щелкните элемент **Параметры логирования**, чтобы открыть диалоговое окно для выбора типов событий, подлежащих записи в журнал задач Discovery.



Включить или отключить запись определенных типов событий можно, установив или сняв соответствующие флажки:

- **Информация** - Выполнено определенное действие.
- **Успех** - Задача или операция завершена успешно.
- **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
- **Ошибка** - Произошла ошибка.

Примечание
Успешные события записываются всегда, поэтому флажок Успех установлен и не может быть снят.

Настройка сообщений для алертов и оповещений

Сетевые администраторы, а также пользователи сканируемых компьютеров могут получать уведомления о некоторых событиях. Предусмотрены два вида уведомлений:

- **Тревожные оповещения (алерты)** - Сообщения, отправляемые Cyber Protego Agent Discovery по протоколам SMTP или SNMP, или передаваемые на сервер syslog. Тревожные алерты существенно упрощают администраторам контроль процессов сканирования и обеспечивают оперативное уведомление о фактах обнаружения критического контента.
- **Пользовательские оповещения** - Системные сообщения, отображаемые текущим пользователям на сканируемых компьютерах, во всплывающем окне рядом с системными часами на панели задач. Пользовательские оповещения появляются, когда Cyber Protego Agent Discovery обнаруживает контент, совпадающий с действующими правилами обнаружения.

  Примечание
  Пользовательские оповещения отображаются только при сканировании посредством агента Discovery. При сканировании без агента алерта пользователей отсутствуют.

В узле **Настройки сервера Discovery** предоставляется возможность задать сообщения для алертов (тревожных алертов) и пользовательских алертов.

Чтобы настроить e-mail сообщение для алертов

1. Дважды щелкните **E-mail сообщение для алертов** в узле **Настройки сервера Discovery**.

   - или -

   Щелкните правой кнопкой мыши **E-mail сообщение для алертов** в узле **Настройки сервера Discovery**, и затем выберите команду **Свойства**.

   Появится диалоговое окно “E-mail сообщение для алертов”.
2. В диалоговом окне **E-mail сообщение для алертов** отредактируйте шаблон сообщения, затем нажмите кнопку **OK**.

   Шаблон содержит следующие данные:

   - **Тема письма** - Текст в строке **Тема** почтового сообщения. Текст по умолчанию: “Алерт Cyber Protego Discovery”.
   - **Тело письма** - Текст почтового сообщения. Cyber Protego может отправлять сообщение как в виде простого текста, так и в HTML. Текст сообщения совпадает в обоих шаблонах и содержит статичный текст и макросы. Статичный текст по умолчанию: “Произошло следующее событие”.

   В строке **Тема письма** и/или в тексте сообщения можно использовать следующие стандартные макросы:

   - %EVENT_TYPE% - Класс события (**Успех** для действия, успешно примененного к обнаруженному контенту, либо **Отказ**, если действие не удалось применить).
   - %COMP_NAME% - Имя компьютера, на котором был обнаружен файл с искомым контентом.
   - %COMP_FQDN% - Полное доменное имя компьютера, на котором был обнаружен файл с искомым контентом.
   - %COMP_IP% - Список всех IP-адресов компьютера, разделенных запятой.
   - %DATE_TIME% - Дата и время, когда искомый контент было бнаружен. Дата и время указываются в соответствии с региональными и языковыми настройками на клиентском компьютере.
   - %ACTION% - Наименование действия, примененного к обнаруженному контенту (файлу).
   - %NAME% - Имя файла, к которому было применено действие.
   - %REASON% - Причина возникновения события (имя правила, сработавшего на файле).
   - %SUMMARY_TABLE% - Сводная таблица, содержащая множество событий, случившихся за определенный отрезок времени.

   Эти макросы заменяются на фактические значения во время создания сообщения.
3. С помощью опций **Формат сообщения** выберите требуемый формат сообщения - **Текст** или **HTML**.
4. При необходимости, нажмите кнопку **Восстановить умолчания** для восстановления шаблона по умолчанию или кнопку **Загрузить** для загрузки ранее сохраненного шаблона.

   Загрузить шаблон можно из текстового файла с разделителем-табуляцией. Файл может содержать простой текст или HTML.

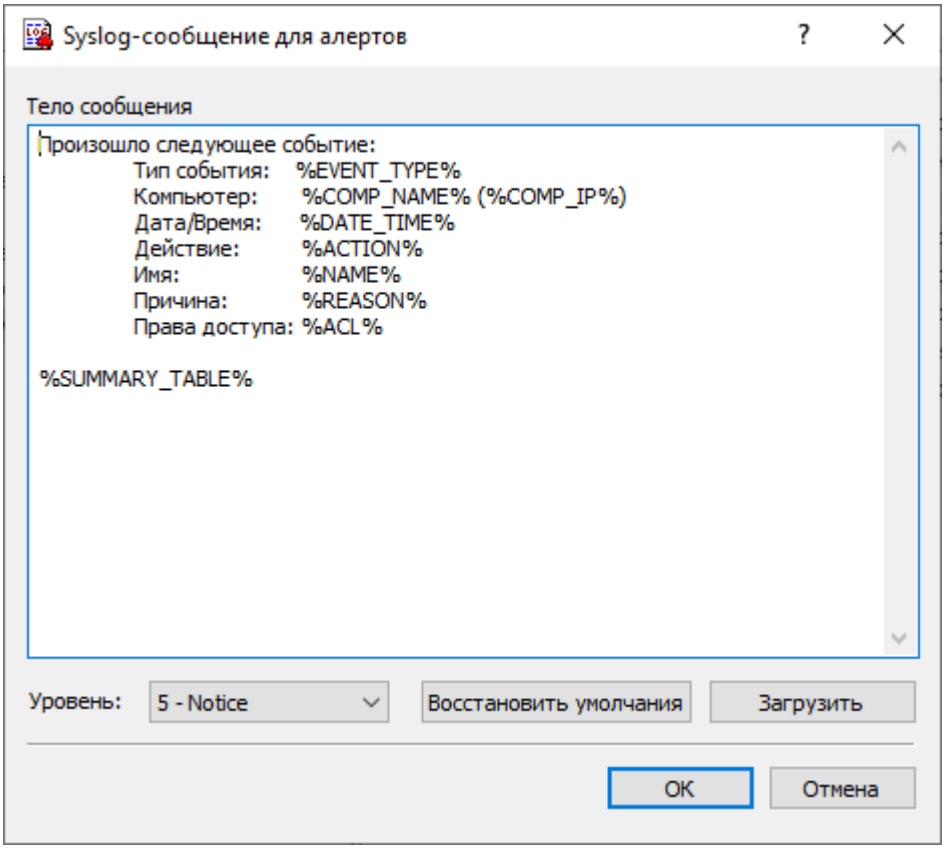
Чтобы настроить Syslog-сообщение для алертов

1. Дважды щелкните **Syslog-сообщение для алертов** в узле **Настройки сервера Discovery**.

   - или -

   Щелкните правой кнопкой мыши на **Syslog-сообщение для алертов** в узле **Настройки сервера Discovery**, и затем выберите команду **Свойства**.

   Появится диалоговое окно “Syslog-сообщение для алертов”.



2. В диалоговом окне **Syslog-сообщение для алертов** отредактируйте шаблон сообщения, затем нажмите кнопку **OK**.

   Шаблон содержит следующие данные:

   - **Тело сообщения** - Текст, отображаемый в syslog-сообщении, содержит статичный текст и макросы. Статичный текст по умолчанию: “Произошло следующее событие”.

   В теле сообщения можно использовать следующие макросы:

   - %EVENT_TYPE% - Класс события (**Успех** для действия, успешно примененного к обнаруженному контенту, либо **Отказ**, если действие не удалось применить).
   - %COMP_NAME% - Имя компьютера, на котором был обнаружен файл с искомым контентом.
   - %COMP_FQDN% - Полное доменное имя компьютера, на котором был обнаружен файл с искомым контентом.
   - %COMP_IP% - Список всех IP-адресов компьютера, разделенных запятой.
   - %DATE_TIME% - Дата и время, когда искомый контент был обнаружен. Дата и время указываются в соответствии с региональными и языковыми настройками на клиентском компьютере.

- %ACTION% - Наименование действия, примененного к обнаруженному контенту (файлу).
- %NAME% - Имя файла, к которому было применено действие.
- %REASON% - Причина возникновения события (имя правила, сработавшего на файле).
- %SUMMARY_TABLE% - Сводная таблица, содержащая множество событий, случившихся за определенный отрезок времени.

Эти макросы заменяются на фактические значения во время создания сообщения.

3. Задайте степень серьезности сообщения, выбрав подходящее значение из списка **Уровень**.
4. При необходимости, нажмите кнопку **Восстановить умолчания** для восстановления шаблона по умолчанию или кнопку **Загрузить** для загрузки ранее сохраненного шаблона.
   Загрузить шаблон можно из файла, содержащего простой текст с табуляцией в качестве разделителя.

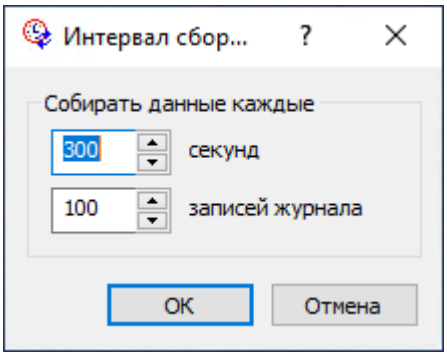
Чтобы настроить Сообщение оповещения об обнаружении

1. Дважды щелкните **Сообщение оповещения об обнаружении** в узле **Настройки сервера Discovery**.
   Появится диалоговое окно “Сообщение оповещения об обнаружении”.
2. В диалоговом окне **Сообщение оповещения об обнаружении** задайте заголовок и текст сообщения. Это сообщение отображается в виде всплывающего окна в системной области уведомлений сканируемого компьютера для всех пользователей, которые в данный момент используют этот компьютер.
   Помимо статического текста, в тексте сообщения можно использовать следующие макросы:
   - %DATA% - Имя файла, на котором сработало правило обнаружения.
   - %ACTION_TAKEN% - Имя действия (действий), которые были применены к обнаруженному контенту (файлу).

Примечание
Сообщение об обнаружении не отображается в режиме сканирования без агента. В случае сканирования данных на терминальном сервере, такое сообщение будет отображено всем подключенным в данный момент пользователям.

Изменение интервала сбора данных

Предусмотрена возможность настройки интервала, через который Агент Discovery уведомляет Сервер Discovery о наличии новых данных для передачи на сервер. Для изменения параметров сбора данных дважды щелкните **Интервал сбора данных** в узле **Настройки сервера Discovery**. Появится диалоговое окно **Интервал сбора данных**.



В поле **Собирать данные каждые** задайте время в секундах, которое должно пройти с момента старта задачи обнаружения и до момента, когда агенты должны начинать уведомлять Сервер Discovery о наличии новых данных. Значение по умолчанию равно 300 секундам.

Также возможно указать количество записей в журнале протоколирования, которое должно быть накоплено, прежде чем агенты Discovery будут уведомлять Сервер Discovery о наличии новых данных. В процессе своей работы агенты Discovery создают в журнале записи о различных событиях. Администратор сервера Discovery может задавать дополнительные правила для протоколирования, указывая на необходимость добавления новых записей в журнал в случае обнаружения определенного контента. Данный параметр определяет порог количества записей в журнале, по достижении которого агенты Discovery будут уведомлять Сервер Discovery о наличии новых данных, в свою очередь Сервер Discovery будет собирать данные с таких агентов. Значение по умолчанию равно 100 записям журнала.

Условия передачи данных по времени в секундах или по количеству записей в журнале используются совместно. Данные будут переданы на сервер, как только сработает любое из двух условий.

Включение проверки содержимого двоичных файлов

Параметр **Проверка содержимого бинарных файлов** позволяет проверять текстовый контент, содержащийся в произвольных двоичных файлах. Когда этот параметр отключен, Cyber Protego выполняет обнаружение контента на основе ключевых слов и шаблонов только для текста в кодировке Unicode, хранящегося в известных типах файлов.

Когда этот параметр включен, Cyber Protego выполняет обнаружение контента на основе ключевых слов и шаблонов для текста, содержащегося в любых двоичных файлах, независимо от кодировки текста (Unicode или не-Unicode). В этом случае обнаружение контента может занять значительно больше времени.

Примечание
Данный параметр влияет на правила обнаружения контента, в которых используются группы ключевых слов, группы шаблонов и/или содержащие их составные контентные группы. Подробнее о правилах обнаружения контента см. в разделе Правила и действия.

Чтобы включить или отключить этот параметр, дважды щелкните элемент **Проверка содержимого бинарных файлов** в списке **Настройки сервера Discovery**, или щелкните этот элемент правой кнопкой мыши и выберите команду **Включить** или **Выключить**.

Алерты

Предусмотрены следующие параметры алертов:

- **SNMP** – позволяет настроить передачу алертов по протоколу SNMP.
- **SMTP** – позволяет настроить доставку алертов по электронной почте через SMTP-сервер.
- **Syslog** – позволяет настроить перенаправление алертов на сервер syslog.
- **Параметры повторной доставки** – позволяет задать действия сервера при сбое доставки алертов.

Чтобы начать настройку параметра, дважды щелкните этот параметр, или щелкните его правой кнопкой мыши и используйте команды в появившемся контекстном меню.

Общая информация

При сканировании компьютеров Cyber Protego Discovery может уведомлять сетевых администраторов об определенных событиях с помощью алертов. Можно настроить алерта на автоматическое уведомление в случае, если агент сканирования обнаруживает контент, совпадающий с одним из заданных правил обнаружения. алерт в реальном времени упрощает сетевое администрирование и помогает быстрее и эффективнее реагировать на инциденты безопасности и нарушения политик.

Агенты Discovery могут отправлять алерты, уведомляющие администраторов об обнаружении контента. Алерты могут отправляться адресатам по электронной почте или через SNMP-уведомления. Кроме того, алерта могут отправляться на сервер syslog.

Чтобы сервер Cyber Protego Search and Discovery Server мог отправлять тревожные алерты, необходимо выполнить следующие действия.

- Выберите способ доставки алертов при возникновении условий срабатывания: через SNMP-уведомления, по электронной почте или через syslog.
- Чтобы получать алерты через SNMP-уведомления, настройте на сервере Cyber Protego Search and Discovery Server поддержку SNMP и укажите SNMP-сервер, на который следует отправлять уведомления. Подробнее см. в разделе Настройки алертов: SNMP.

  Примечание
  Здесь и далее предполагается, что вы знакомы с протоколом SNMP (Simple Network Management Protocol) и соответствующими принципами управления.

- Чтобы получать алерты по электронной почте, настройте почтовые уведомления, указав SMTP-сервер, настройки уведомления и шаблоны сообщений. Подробнее см. в разделе Настройки алертов: SMTP.

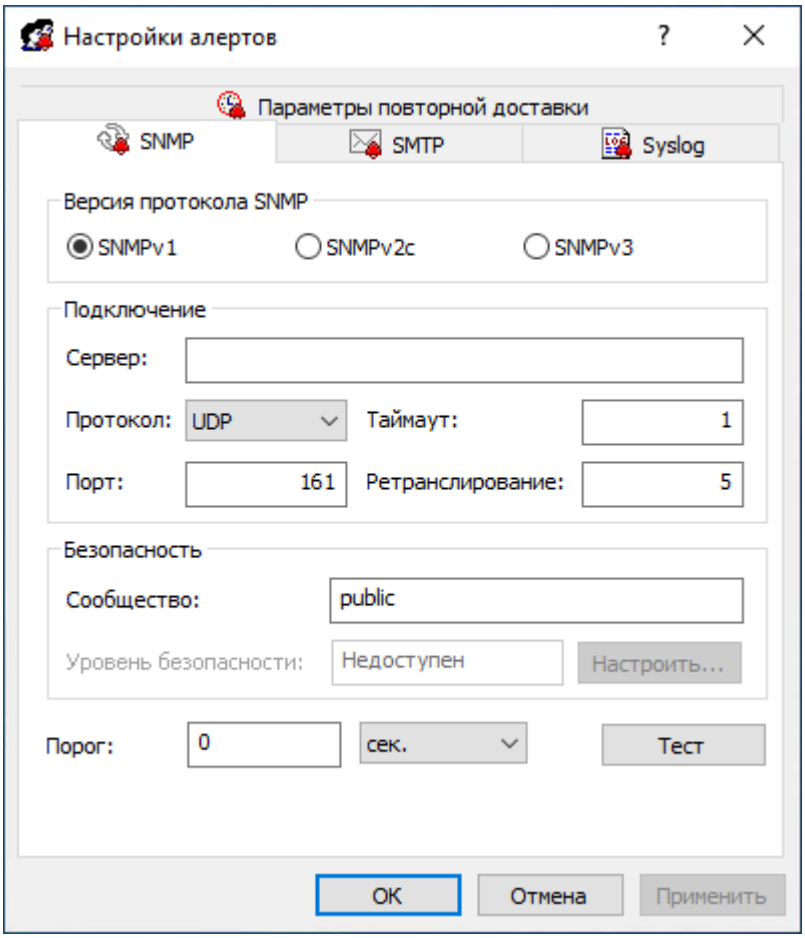
- Чтобы получать алерты через syslog, настройте syslog на сервере Cyber Protego Search and Discovery Server и укажите сервер syslog, на который следует отправлять алерты. Подробнее см. в разделе Настройки алертов: Syslog.

  Примечание
  Здесь и далее предполагается, что вы знакомы с протоколом syslog и соответствующими принципами управления.

- Настройте действия сервера при сбое доставки алертов, в том числе количество и периодичность повторных попыток, а также срок хранения недоставленного сообщения в очереди на отправку. Подробнее см. в разделе Настройки алертов: параметры повторной доставки.

Настройки алертов: SNMP

На вкладке **SNMP** диалогового окна **Настройки алертов** можно настроить поддержку SNMP в Search and Discovery Server.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой **SNMP** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **SNMP**.

Cyber Protego поддерживает протоколы SNMPv1, SNMPv2c и SNMPv3. Можно настроить Search and Discovery Server на автоматическую рассылку алертов на указанный SNMP-сервер при возникновении условий срабатывания. Алерты отправляются только при соблюдении следующих условий:

- SNMP-сервер настроен на получение SNMP traps (уведомлений).
- Удаленный компьютер, на котором работает SNMP-сервер, доступен со всех компьютеров, где выполняются задачи обнаружения (посредством агента) или с сервера (при сканировании без использования агента).
- Включена рассылка алертов через SNMP-уведомления.

Заполните вкладку **SNMP** следующим образом:

- **Версия протокола SNMP** - Выберите версию протокола SNMP в соответствии с требованиями вашего SNMP-сервера. Возможные варианты: **SNMPv1**, **SNMPv2c** и **SNMPv3**.
- **Подключение** - Укажите информацию об SNMP-сервере:
  - **Сервер** - SNMP-сервер, на который будут отправляться уведомления. В поле **Сервер** введите имя узла или IP-адрес SNMP-сервера.
  - **Протокол** - Транспортный протокол для передачи данных между Cyber Protego и SNMP-сервером. Возможные варианты: **UDP** и **TCP**.
  - **Таймаут** - Промежуток времени, в течение которого Cyber Protego ожидает ответа от SNMP-сервера (в секундах) перед повторной отправкой пакета данных. Значение по умолчанию - 1 секунда.
  - **Порт** - Порт, по которому SNMP-сервер должен получать SNMP-уведомления. Порт умолчанию - используется порт 161.
  - **Ретранслирование** - Количество повторных запросов на SNMP-сервер, если сервер не отвечает (относится только к протоколу **TCP**). Количество повторных запросов по умолчанию - 5.
- **Безопасность** - Задайте параметры безопасности SNMP:
  - **Сообщество** (если выбран SNMPv1 или SNMPv2c) - Имя группы SNMP для аутентификации на SNMP-сервере. Значение по умолчанию: public.
  - **Имя пользователя** (если выбран SNMPv3) - Имя учетной записи пользователя для аутентификации на SNMP-сервере. Чтобы задать имя пользователя, нажмите кнопку **Настроить**, расположенную рядом с полем **Уровень безопасности**. Если аутентификация не требуется, имя пользователя можно не задавать.

- **Уровень безопасности** (если выбран SNMPv3) - Значение, указывающее уровень безопасности соединения с SNMP-сервером. Возможные значения:
  - **Нет защиты** - Отсутствие аутентификации и шифрования.
  - **Аутентификация** - Наличие аутентификации, отсутствие шифрования.
  - **Аутентификация и конфиденциальность** - Наличие как аутентификации, так и шифрования.
- **Настроить** (если выбран SNMPv3) - Нажмите кнопку **Настроить**, расположенную рядом с полем **Уровень безопасности**, чтобы задать следующие параметры:
  - **Имя пользователя** - Укажите имя учетной записи пользователя для аутентификации на SNMP-сервере. Если аутентификация не требуется, имя пользователя можно не задавать.
  - **Имя контекста** - Укажите имя контекста, если SNMP-сервер требует контекст SNMP.
  - **ID контекстного движка** - Укажите идентификатор контекстного движка, если SNMP-сервер требует контекст SNMP.
  - **Протокол аутентификации** - Выберите протокол для шифрования аутентификации на SNMP-сервере. Возможные варианты:
    - **Нет** - Уровень безопасности **Нет защиты**.
    - **HMAC-SHA** - Уровень безопасности **Аутентификация** или **Аутентификация и конфиденциальность**, в зависимости от настройки параметра **Протокол конфиденциальности**.
  - **Пароль/ Подтверждение пароля** - Введите пароль учетной записи пользователя, используемой для аутентификации на SNMP-сервере (относится к параметру **Протокол аутентификации**).
  - **Протокол конфиденциальности** - Выберите протокол шифрования данных при взаимодействии с SNMP-сервером. Возможные варианты:
    - **Нет** - Уровень безопасности **Нет защиты** или **Аутентификация**, в зависимости от настройки параметра **Протокол аутентификации**.
    - **CBC-AES-128** - Security level of **Authentication and Privacy**, requires the **Authentication protocol** setting other than **None**.
  - **Пароль/ Подтверждение пароля** - Введите пароль для шифрования данных (относится к параметру **Протокол конфиденциальности**).

- **Порог** - Задайте временной интервал (в часах, минутах или секундах) для консолидации событий при отправке алертов. Cyber Protego консолидирует похожие события, произошедшие в течение порогового времени, и создает объединенное событие, если выполняются следующие условия:
  a. События относятся к одному типу - **Успех**, если действия успешно выполнены для обнаруженного контента, или **Отказ**, если действия были не успешны.
  b. Значения полей **Причина** и **Компьютер** совпадают.
  Значение по умолчанию - 0 секунд.

- **Тест** - Отправьте тестовое SNMP-уведомление, чтобы проверить правильность настройки Cyber Protego. В результате тестовой операции отобразится одно из двух сообщений:

- Тест может быть выполнен успешно, т.е. пробное SNMP-уведомление было отправлено с настроенными для него параметрами. В этом случае сообщение будет следующим: “Тестовое алерт SNMP успешно отправлен.”
- Тест может быть не выполнен, т.е. пробное SNMP-уведомление отправить не удалось. В этом случае сообщение будет следующим: “Тестовое алерт SNMP не был отправлен из-за ошибки: <описание ошибки>.”

SNMP-уведомления от сервера Cyber Protego Discovery представляются в формате MIB (Management Information Base). MIB для Cyber Protego Discovery имеет идентификатор объекта (OID) 1.3.6.1.4.1.57836 iso.org.dod.internet.private.enterprise.CyberprotectLLC и содержит следующие узлы:

- products(1)
- discoveryAgent(1)
- alerts(1) - Этот узел содержит по одному экземпляру каждого из следующих MIB-объектов:
  - eventType(1) - Класс события (Успех для успешной попытки либо Отказ для неудачной попытки). Обратите внимание, что значение eventType отображается в виде числа, а не строки: 8 означает успешную попытку, 16 - неудачную.
  - computerName(2) - Имя компьютера, от которого получено событие.
  - action(3) - Тип действия пользователя.
  - name(4) - Имя обнаруженного объекта.
  - reason(5) - Причина возникновения события.
  - datetime(6) - Дата и время (в формате RFC3339) события обнаружения контента.

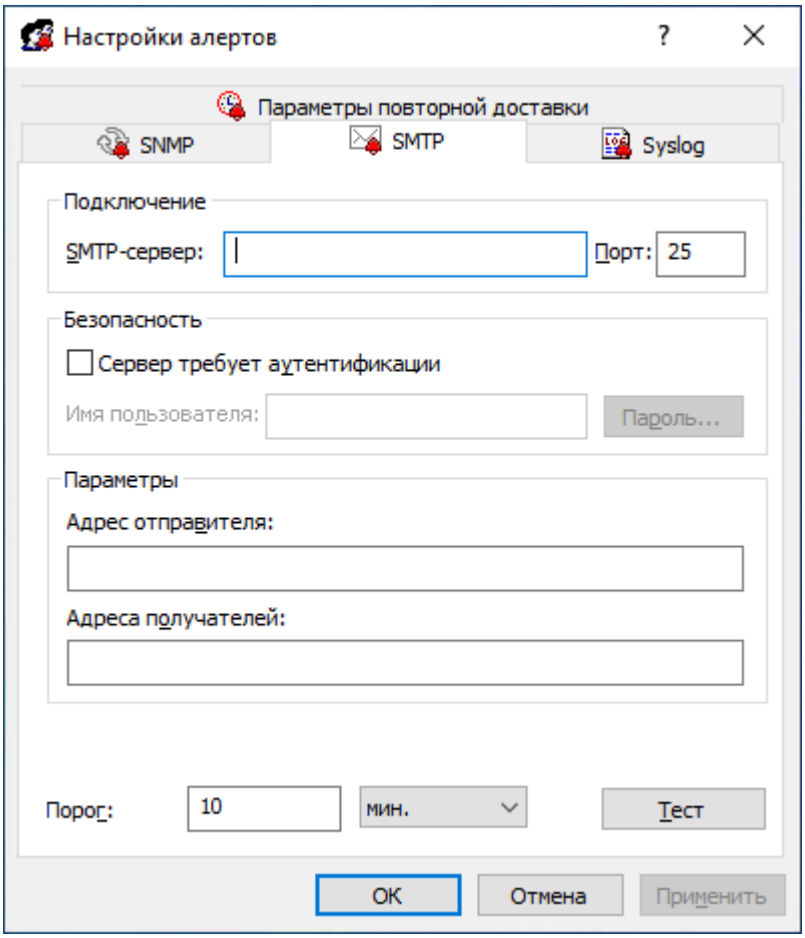
Примечание
Данные MIB-объекты соответствуют полям в журнале задач (описание полей см. в разделе Просмотрщик журнала задач).

SNMP-уведомление рассылается каждый раз, когда происходит событие, ассоциированное с тревожным алертм. Ниже приводится пример тревожного алерта (оповещения), направленного по протоколу SNMP при обнаружении определенного контента.

Specific: 1
Message reception date: 21.02.2014
Message reception time: 13:25:34.862
Time stamp: 274 days 06h:37m:07s.29th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
Address: 10.10.30.16
Port: 59467
Manager
Address: 192.168.209.1
Port: 0
Community: public
SNMPv1 agent address: 10.10.30.16
Enterprise: enterprises.60000
Bindings (6)
Binding #1: enterprises.60000.1.2.1.1 *** (gauge) 8
Binding #2: enterprises.60000.1.2.1.2 *** (octet string) WIN7X64_DLADGLI
Binding #3: enterprises.60000.1.2.1.3 *** (octet string) Log, Alert
Binding #4: enterprises.60000.1.2.1.4 *** (octet string) C:\Documents\Research.docx
Binding #5: enterprises.60000.1.2.1.5 *** (octet string) Rule: "Secret data" (Any keyword matched)
Binding #6: enterprises.60000.1.2.1.6 *** (octet string) 2014-02-21T09:25:34Z

Настройки алертов: SMTP

На вкладке **SMTP** диалогового окна **Настройки алертов** можно настроить отправку уведомлений по электронной почте.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой **SMTP** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **SMTP**.

Для передачи алертов посредством почтовых сообщений Cyber Protego использует протокол SMTP. Можно настроить автоматическую рассылку тревожных алертов на указанные адреса электронной почты при срабатывании заданных условий.

Для настройки почтовых алертов заполните вкладку **SMTP** следующим образом:

- **Подключение** - Укажите данные почтового (SMTP) сервера:
  - **SMTP-сервер** - Имя или IP-адрес почтового сервера.
  - **Порт** - Номер порта SMTP-сервера. Порт по умолчанию - 25.

Примечание
Поддерживаются как незащищенные, так и защищенные (SSL) соединения с почтовым сервером. Cyber Protego автоматически определяет и устанавливает требуемый тип соединения.

- **Безопасность** - Если для соединения с почтовым сервером требуется проверка подлинности, установите флажок **Сервер требует аутентификации** и введите имя и пароль пользователя почтового сервера в соответствующие поля диалогового окна.
- **Параметры** - Укажите отправителя и получателей сообщения:
  - **Адрес отправителя** - Почтовый адрес, с которого будут рассылаться сообщения . Как правило, он совпадает с именем пользователя почтового сервера (например, user@mailserver.com). Адрес отправителя отображается в поле **От** почтового сообщения.
  - **Адреса получателей** - Адреса электронной почты, на которые требуется отправлять сообщения. Можно ввести несколько адресов, разделяя их запятой (,) или точкой с запятой (;).
- **Порог** - Задайте временной интервал (в часах, минутах или секундах) для консолидации событий при отправке алертов. Cyber Protego консолидирует похожие события, произошедшие в течение порогового времени, и создает объединенное событие, если выполняются следующие условия:
  a. События относятся к одному типу - **Успех** для успешно выполненных действий для обнаруженного контента, или **Отказ**, если действия были не успешны.
  b. Значения полей **Причина** и **Компьютер** совпадают.
  Значение по умолчанию - 10 минут.
- **Тест** - Отправьте тестовое сообщение, чтобы проверить правильность настройки Cyber Protego. В результате тестовой операции отобразится одно из двух сообщений:
  - Если тест выполнен успешно, т.е. пробное сообщение отправлено с настроенными для него параметрами, сообщение будет следующим: “Тестовое алерт SMTP успешно отправлен.”
  - Если тест не выполнен, т.е. пробное сообщение отправить не удалось, сообщение будет следующим: “Тестовое алерт SMTP не был отправлен из-за ошибки: <описание ошибки>.”

Ниже приводится пример алерта, доставленного по электронной почте:

Алерт Cyber Protego

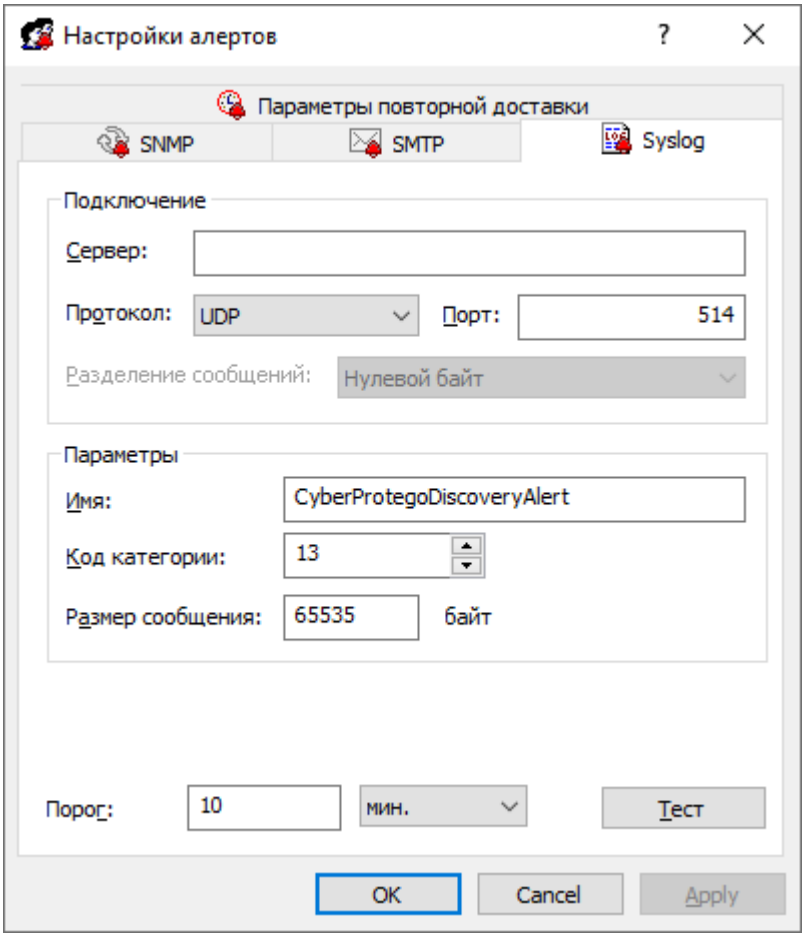
Произошло следующее событие:
Тип события: Успех (8)
Компьютер: WIN7X64_DLADGLI
Дата/время: 02/21/14 12:05:02
Действие: Протоколировать, алерт
Имя: C:\Documents\Research.docx
Причина: Правило: “Закрытые данные” (Совпало: Все ключевые слова)

Примечание

Имена полей в почтовом алерте соответствуют именам полей в журнале задач (описание полей см. в разделе Просмотрщик журнала задач).

Настройки алертов: Syslog

На вкладке **Syslog** диалогового окна **Настройки алертов** можно настроить параметры для отправки алертов на сервер syslog.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой **Syslog** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **Syslog**.

Можно настроить Cyber Protego Search and Discovery Server на автоматическую отправку тревожных алертов на указанный сервер syslog при возникновении условий срабатывания. Отправка алертов происходит только при соблюдении следующих условий:

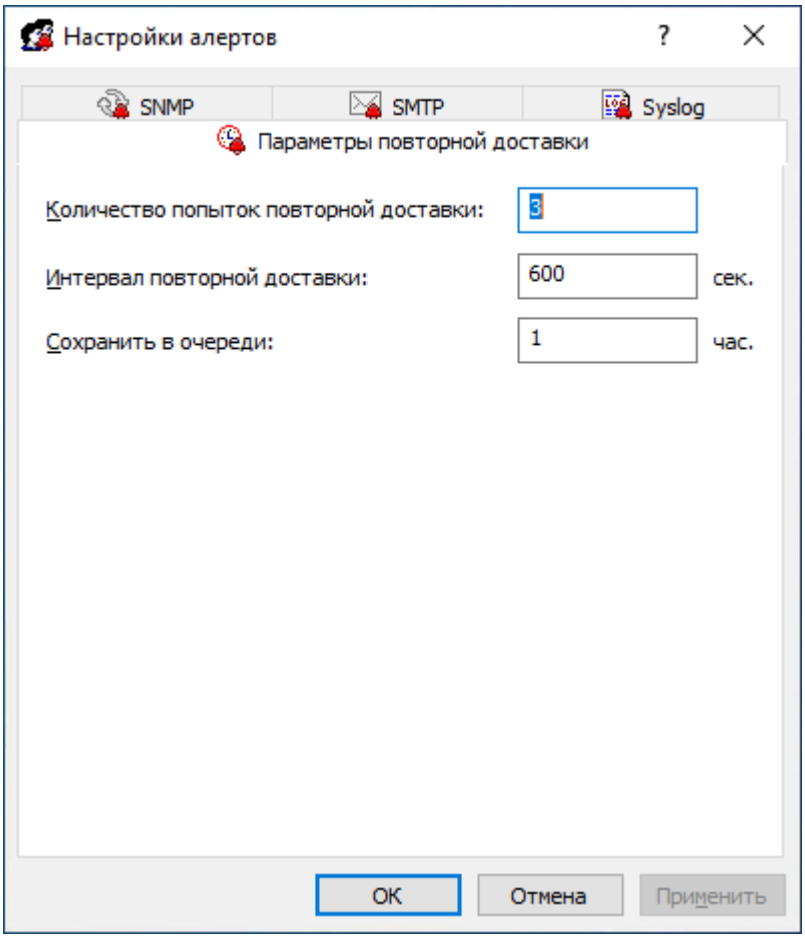
- Сервер syslog настроен и готов к приему алертов.
- Удаленный компьютер, на котором запущен сервер syslog, доступен со всех компьютеров, на которых выполняются задачи обнаружения контента.
- Настроена отправка тревожных алертов на сервер syslog.

Чтобы настроить отправку тревожных алертов на сервер syslog, заполните вкладку **Syslog** следующим образом:

- **Подключение** - Введите информацию о сервере syslog:
  - **Сервер** - Доменное имя или IP адрес сервера syslog.
  - **Протокол** - Протокол доступа к серверу syslog, **TCP** или **UDP**. По умолчанию выбран протокол **UDP**.
  - **Порт** - Номер порта для доступа к серверу syslog. Порт по умолчанию - 514.
  - **Разделение сообщений** - Способ формирования сообщений для протокола **TCP**. Можно выбрать: **Нулевой байт**, **LF**, **CR+LF** или Длина сообщения.
- **Параметры** - Задайте следующие параметры подключения:
  - **Имя** - Уникальное имя для канала связи с сервером syslog. По умолчанию используется имя CyberProtegoDiscoveryAlert.
  - **Код категории** - Одно из стандартных значений сервера syslog (от 0 до 23) для указания типа программы, которая записывает сообщения в журнал.
  - **Размер сообщения** - Размер syslog-сообщения, в байтах. Размер по умолчанию - 65535 байт.
- **Порог** - Задайте временной интервал (в часах, минутах или секундах) для консолидации событий при отправке алертов. Cyber Protego консолидирует похожие события, произошедшие в течение порогового времени, и создает объединенное событие, если выполняются следующие условия:
  a. События относятся к одному типу - **Успех** для успешно выполненных действий для обнаруженного контента, или **Отказ**, если действия были не успешны.
  b. Значения полей **Причина** и **Компьютер** совпадают.
  Значение по умолчанию - 10 минут.
- **Тест** - Отправьте тестовое сообщение, чтобы проверить правильность настройки. В результате тестовой операции отобразится одно из двух сообщений:
  - Если тест выполнен успешно, т.е. пробное сообщение отправлено с настроенными для него параметрами, сообщение будет следующим: “Тестовое алерт Syslog успешно отправлен.”
  - Если тест не выполнен, т.е. пробное сообщение отправить не удалось, сообщение будет следующим: “Тестовое алерт Syslog не был отправлен из-за ошибки: <описание ошибки>.”

Настройки алертов: Параметры повторной доставки

Используйте вкладку **Параметры повторной доставки** в диалоговом окне **Настройки алертов** чтобы настроить действия сервера в случае сбоя доставки алертов.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой мыши **Параметры повторной доставки** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **Параметры повторной доставки**.

Cyber Protego создает и рассылает тревожные алерты в момент возникновения соответствующих им событий. Если при первой попытке Cyber Protego не сможет отправить алерт, создается очередь для хранения не доставленных алертов, которые через определенный промежуток времени высылаются повторно. Можно указать для Cyber Protego максимальное количество попыток рассылки алертов, задать интервал между попытками отправки, а также срок хранения не доставленных алертов в очереди.

Заполните вкладку **Параметры повторной доставки** следующим образом:

- **Количество попыток повторной доставки** - Укажите максимальное количество попыток отправки алертов, выполняемых Cyber Protego Agent, если первая попытка окончилась неудачей. Если алерт не удалось отправить в первый раз, оно попадает в очередь и помечается

как не доставленное. После каждой неудачной попытки счетчик увеличивается на единицу. Этот параметр должен содержать число от 0 до 999. Значение по умолчанию - 3.

По достижении лимита попыток Cyber Protego Agent регистрирует ошибку в своем журнале аудита (“<название_канала> для алертов недоступно и временно отключено из-за ошибки: <код_ошибки> - <описание_ошибки>”) и временно прекращает передачу данных по каналу рассылки алертов (SNMP, SMTP и/или syslog).

Cyber Protego Agent автоматически попытается восстановить соединение с указанным сервером SNMP, SMTP или syslog при проверке состояния соединения (т.е. есть ли подключение к сети или нет). После восстановления соединения Cyber Protego Agent возобновит рассылку алертов.

Для обычного и автономного профилей можно задать разные значения этого параметра.

- **Интервал повторной доставки** - Укажите, сколько времени (в секундах) Cyber Protego Agent будет ждать перед повторной отправкой не доставленного алерта. Значение должно быть в интервале от 10 до 3600 (по умолчанию 600 секунд).
- **Сохранить в очереди** - Укажите период времени (в часах), в течение которого не доставленные алерты должны храниться в очереди до того, как будут удалены. Для всех каналов рассылки используется одна и та же очередь (SNMP, SMTP и/или syslog).
  Для этого параметра может быть установлено значение от 1 до 999 часов. Значение по умолчанию - 1 час.

  Данный параметр можно задать только для обычного профиля. Для обоих профилей (обычного и автономного) используется одно и то же значение.

Сброс настроек алертов в значения по умолчанию

В любой момент можно сбросить настройки алертов в значения по умолчанию («Не определено»). Чтобы сбросить все настройки уведомлений, щелкните правой кнопкой мыши **Алерты** в дереве консоли и выберите в контекстном меню пункт **Отменить определение**. Эта команда сбрасывает все настройки алертов в значения по умолчанию («Не определено»).

Сброс индивидуальных настроек

Можно также сбросить индивидуальные настройки, например **SNMP**, **SMTP**, **Syslog** и **Параметры повтора доставки**. Для этого выберите **Алерты** в дереве консоли и щелкните правой кнопкой мыши конкретный пункт в панели сведений. Выберите в контекстном меню **Отменить определение**, чтобы сбросить выбранный параметр.

Сканирование рабочих станций и сетевых устройств

Сервер Discovery

Сервер Discovery сканирует компьютеры пользователей и хранилища данных, используя настраиваемые правила для обнаружения определенного контента. Сканирование может сопровождаться различными действиями в зависимости от настроек обнаружения, например можно предоставлять или запрещать доступ к контенту, удалять или шифровать контент, оповещать администраторов или уведомлять пользователей компьютеров.

Основу настроек обнаружения составляют так называемые “подразделения”, определяющие область сканирования. В область сканирования могут входить как локальные диски и папки компьютера, так и общие сетевые ресурсы с доступом по SMB. Подразделениям назначаются правила обнаружения, а также действия, которые необходимо выполнять при обнаружении контента, соответствующего этим правилам.

После настройки модулей, правил и действий администратор может настраивать и запускать задачи обнаружения. При выполнении каждая такая задача сканирует свои подразделения и применяет указанные правила и действия. Кроме того, задача создает отчеты и регистрирует события, давая возможность просмотра и анализа результатов обнаружения и выполненных действий.

Порядок настройки обнаружения можно кратко изложить следующим образом:

1. Настроить подразделения, указав места расположения данных для сканирования. Подробнее см. в разделе Подразделения.
2. Задать правила обнаружения и действия, которые необходимо выполнять при обнаружении соответствующего контента. Подробнее см. в разделе Правила и действия.
3. Настроить задачи обнаружения и запланировать их выполнение. Подробнее см. в разделе Задачи.

Подразделения

Подразделение является базовой сущностью в Cyber Protego Discovery, используемой для сканирования и обнаружения определенного контента. Подразделение состоит из одного или более компьютеров, имеющих следующие общие свойства:

- Общие учетные записи.
- Общие настройки области сканирования (заданные включающими и исключающими фильтрами).
- Общий тип сканирования.

Все подразделения, которые в данный момент имеются на сервере, отображаются в узле консоли **Search and Discovery Server** > **Сервер Discovery** > **Подразделения**.

Если в дереве консоли выбран узел **Подразделения**, на панели сведений отображается список всех подразделений, имеющихся на сервере в данный момент.

Панель сведений отображает список со следующими сведениями по каждому подразделению:

- **Имя подразделения** - Имя, идентифицирующее данное подразделение.
- **Тип подразделения** - Целевое назначение подразделения: сканирование компьютеров (тип **Компьютеры**) или сканирование узлов Elasticsearch (тип **Узлы Elasticsearch**).

Контекстное меню узла **Подразделения** содержит следующие команды:

- **Создать новое подразделение** - Создать подразделение. Параметры нового подразделения можно задать в диалоговом окне, которое открывает эта команда.
- **Обновить** - Обновить список подразделений с учетом последних изменений.

Контекстное меню подразделения на панели сведений содержит следующие команды:

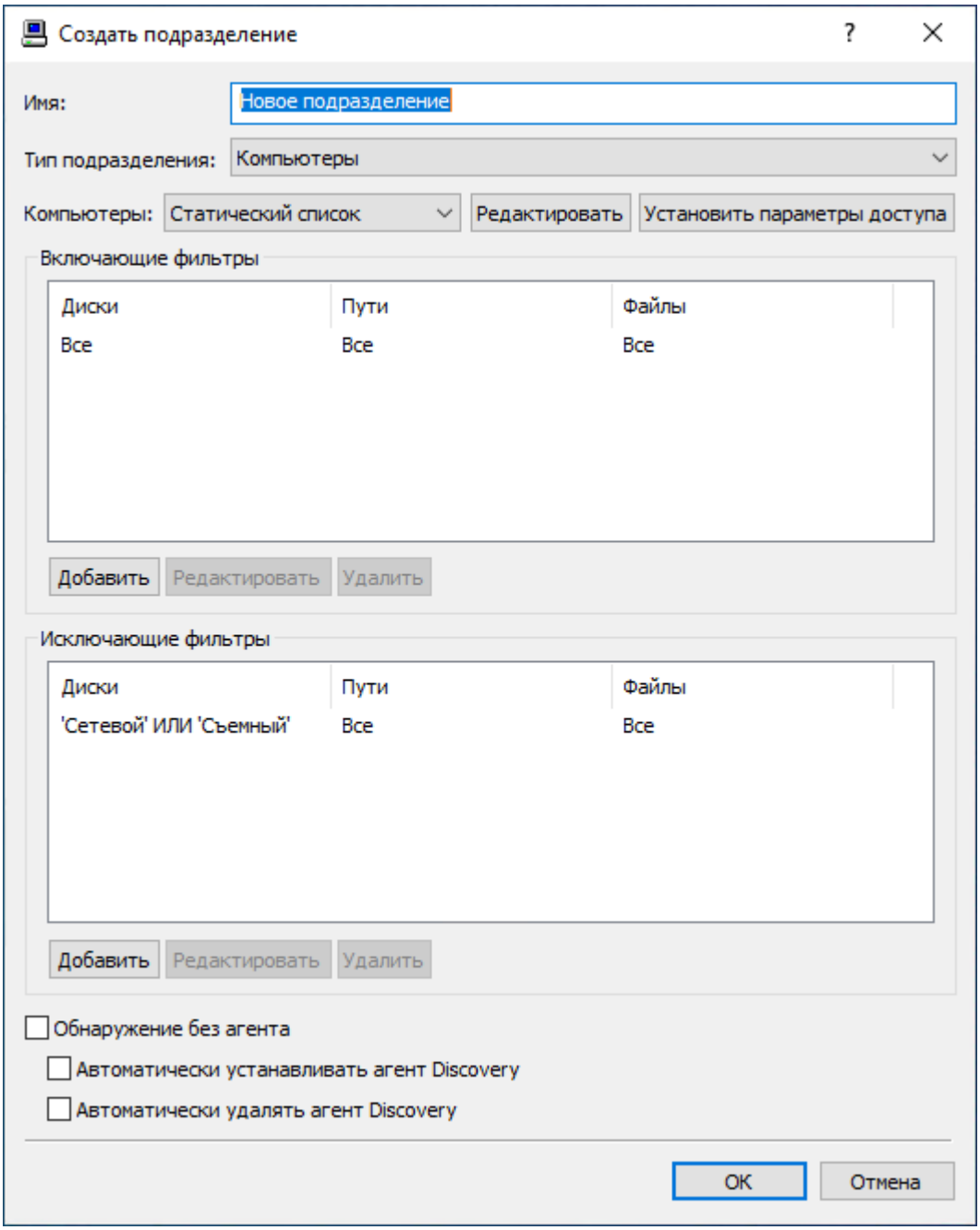
- **Редактировать подразделение** - Просмотреть или изменить параметры подразделения в диалоговом окне, которое открывает эта команда.
- **Дублировать подразделение** - Создать новое подразделение путем копирования параметров выбранного подразделения. Параметры нового подразделения можно редактировать в диалоговом окне, которое открывает эта команда.
  Имя нового подразделения по умолчанию состоит из префикса **Копия**, за которым следует имя выбранного подразделения. При создании двух или более копий к новому имени по умолчанию добавляется числовой суффикс, указывающий номер копии.
- **Редактировать список компьютеров** - Просмотреть или изменить список компьютеров, входящих в состав данного подразделения. Список компьютеров можно редактировать в диалоговом окне, которое открывает эта команда.
- **Удалить подразделение** - Удалить выбранное подразделение.
- **Обновить** - Обновить список подразделений с учетом последних изменений.

Создание подразделения

Чтобы создать подразделение, откройте и заполните диалоговое окно **Создать подразделение**. Это диалоговое окно можно открыть следующим образом:

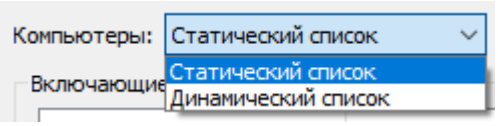
1. В дереве консоли раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Подразделения**.
2. Щелкните правой кнопкой мыши узел **Подразделения** и выберите команду **Создать новое подразделение** в контекстном меню.
   - или -
   Выберите узел **Подразделения** и нажмите кнопку **Создать новое подразделение** на панели инструментов.

Появится диалоговое окно **Создать подразделение**.



Заполните диалоговое окно **Создать подразделение** следующим образом:

- **Имя** - Задайте отображаемое имя для создаваемого подразделения.
- **Тип подразделения** - Для обнаружения файлов на компьютерах и серверах выберите тип подразделения **Компьютеры**. Для обнаружения документов в Elasticsearch выберите тип подразделения **Узлы Elasticsearch**.
  Ниже описывается тип подразделения **Компьютеры**. Описание типа **Узлы Elasticsearch** см. в разделе Подразделения Elasticsearch.
- **Компьютеры** - Задайте список компьютеров для данного подразделения. Доступны два типа списков: **Статический список** и **Динамический список**. Тип списка можно выбрать при создании подразделения. После того, как подразделение создано, изменить тип списка невозможно.

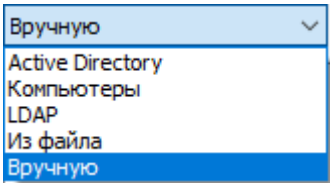


1. **Статический список** - Компьютеры в списке задаются по именам или IP-адресам. Поскольку этот список статический, то даже если какой-либо компьютер более не существует в сети, он будет сканироваться (с созданием события об ошибке), пока запись о нем не будет удалена вручную из этого списка.
   Сканируемые компьютеры задаются в списке справа. Компьютеры, подлежащие сканированию, следует выбрать в левом списке, а затем переместить их в список справа, используя кнопку `>`.

   Для исключения компьютеров из задач сканирования следует выбрать их в правом списке и нажать кнопку `<`.

   Используя кнопки `>>` и `<<`, можно добавлять и удалять все доступные компьютеры за один раз (не нужно по отдельности выделять компьютеры в списках).

   Есть несколько вариантов выбора компьютеров в левом списке:

   - **Active Directory** - Выбор компьютеров из папок (подразделений) службы каталогов Active Directory.
   - **Компьютеры** - Выбор из числа компьютеров, зарегистрированных в локальной сети.
   - **LDAP** - Выбор компьютеров из LDAP-совместимой службы каталогов.
   - **Из файла** - Загрузка заранее подготовленного списка компьютеров из текстового файла с последующим выбором компьютеров. Файл должен содержать список компьютерных имен или IP-адресов по одному имени или адресу на строке. Чтобы открыть файл, нажмите кнопку `...`.
   - **Вручную** - Ввод и выбор компьютеров вручную. Каждое имя или IP-адрес компьютера должно быть введено на отдельной строке. Для перехода на новую строку нажимайте клавишу ENTER.
2. **Динамический список** - В отличие от статического списка, вместо имен компьютеров и/или IP-адресов динамический список содержит путь к контейнеру (например, подразделение) в дереве службы каталогов (такой как Active Directory, Novell eDirectory, OpenLDAP и т. п.). Каждый раз в момент выполнения задачи Сервер Discovery получает список всех компьютеров, которые в настоящий момент времени существуют в контейнере. Таким образом, если какой-либо компьютер был удален из службы каталогов или был перемещен в другой контейнер, то он не будет более сканироваться. И наоборот, если появился новый компьютер, который не существовал в контейнере на момент создания/редактирования задачи, а был добавлен туда позже, то данный компьютер будет сканироваться во время выполнения задачи. Можно выбрать один или несколько контейнеров.

Путь к выбранным контейнерам указывается в поле **Путь**. Выберите контейнеры в дереве щелчком мыши, удерживая нажатой клавишу Shift или Ctrl. Затем нажмите кнопку **Выбрать**. Чтобы отменить выбор контейнера, нажмите красный крестик в поле **Путь**.

Установите флажок **Просматривать вложенные контейнеры**, чтобы разрешить серверу Discovery получать компьютеры из всех вложенных контейнеров, находящихся внутри выбранного контейнера. В противном случае, если флажок Просматривать вложенные контейнеры выключен, то все вложенные контейнеры игнорируются, а список компьютеров формируется только из выбранного контейнера.

Существует два режима работы со агентми каталогов:

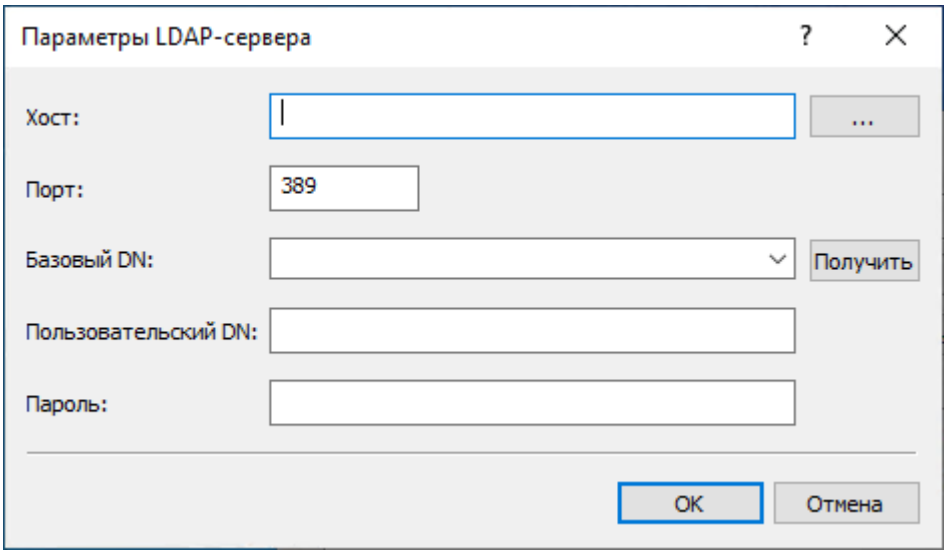
- **Active Directory** - Просмотр дерева Active Directory с выбором нужного контейнера.
  Хотя работать с деревом Active Directory можно и в режиме LDAP (см. ниже), рекомендуется использовать именно специальный режим Active Directory, т.к. в этом случае Сервер Discovery работает со службой каталогов более эффективно и потребляет меньше ресурсов.
  Если для доступа к Active Directory требуется задать данные (пользователь и пароль) альтернативной учетной записи, нажмите на кнопку ··· и укажите необходимое имя пользователя и соответствующий ему пароль.

Примечание
Если альтернативная учетная запись не задана, то для доступа к Active Directory используется учетная запись, от имени которой запущена Cyber Protego Agent Search and Discovery Server. Подробнее см. в разделе Настройка стартовой учетной записи службы сервера.

Установите флажок **Синхронизация**, чтобы разрешить серверу Discovery использовать функцию синхронизации, предоставляемую Active Directory. Это позволяет значительно снизить нагрузку на контроллер домена и быстрее получать список компьютеров в момент выполнения задачи.

Примечание
Чтобы использовать функцию синхронизации, Сервер Discovery должен иметь доступ к Active Directory с правами администратора домена.

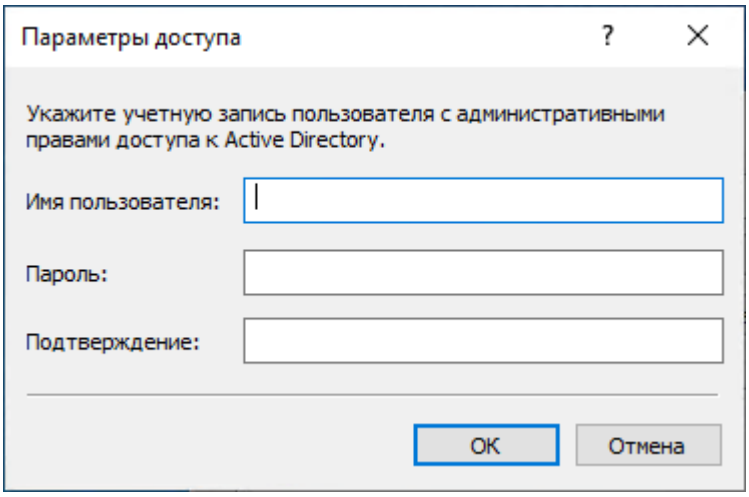
- **LDAP** - Просмотр LDAP-дерева (Lightweight Directory Access Protocol) с выбором нужного контейнера.
  Чтобы настроить подключение к LDAP-серверу, нажмите кнопку ··· и заполните диалоговое окно **Настройки LDAP**.



- **Хост** - Имя или IP-адрес LDAP-сервера, к которому выполняется подключение.
- **Порт** - Номер порта, по которому LDAP-сервер принимает подключения. По умолчанию используется порт 389.
- **Базовый DN** - Начальная точка для просмотра дерева каталогов. Это должно быть действительное DN-имя, например cn=users,o=company,c=US. Если базовый DN не указан, просмотр начинается с корня дерева. Нажмите кнопку **Получить**, чтобы выбрать контекст именования для базового DN.
- **Пользовательский DN**, **Пароль** - DN-имя и пароль пользователя службы каталогов для доступа к LDAP-серверу. Это должно быть быть действительное DN-имя, например cn=admin,o=company,c=US.

Примечание
Если имя пользователя не указано, для доступа к LDAP-серверу используется стартовая учетная запись службы Search and Discovery Server. Подробнее об этой учетной записи см. в разделе Настройка стартовой учетной записи службы сервера.

- **Установить параметры доступа** - При необходимости, нажмите эту кнопку, чтобы указать имя и пароль учетной записи с достаточными правами для доступа к компьютерам из списка. Рекомендуется использовать учетную запись, обладающую правами администратора на всех сканируемых компьютерах.



Установка параметров доступа не является обязательной. Если параметры доступа не установлены, Сервер Discovery получает доступ к удаленным ресурсам посредством учетной записи, под которой запущена Cyber Protego Agent Search and Discovery Server, или использует сертификат Cyber Protego для доступа к Cyber Protego Agent с установленным сертификатом.

Примечание

- Для применения указанных параметров доступа Cyber Protego Agent Search and Discovery Server должна быть запущена под учетной записью с правами локального администратора.
- При использовании базы данных другого сервера Discovery потребуется заново ввести параметры доступа. Поскольку эти параметры зашифрованы защищенным ключом, хранящемся на сервере, они не могут быть расшифрованы другим сервером Discovery, так что их необходимо ввести заново.

- **Включающие фильтры / Исключающие фильтры** - Задайте параметры включающих или исключающих фильтров, которые определяют, какие диски, папки и файлы будут сканироваться. По умолчанию Cyber Protego Discovery сканирует все диски, папки и файлы на компьютере, за исключением съемных носителей и подключенных сетевых устройств.
  Для создания нового фильтра нажмите кнопку **Добавить** под соответствующим списком фильтров. Для добавления включающего или исключающего фильтра служит диалоговое окно **Добавить включающий фильтр** или **Добавить исключающий фильтр** соответственно. Описание этих диалоговых окон см. в разделе Добавление фильтров. Редактировать или удалять ранее созданные фильтры можно нажатием на кнопку **Редактировать** или **Удалить** соответственно.

  Правила внутри фильтра объединяются по ИЛИ. Например, если у включающего фильтра установить флажки **Системный**, **Не системный** и **Съемный, Гибкий и Оптический** в категории **Все диски**, сканироваться будут только указанные типы устройств. Если еще установить флаг Документы, то на указанных устройствах будет сканироваться только папка Документы. При использовании нескольких фильтров они объединяются по ИЛИ, т.е. сканироваться будет область, соответствующая любому из заданных фильтров. Включающие и исключающие фильтры объединяются по И. Дополнительные сведения см. в разделе Создание фильтра: Пример.

- **Обнаружение без агента** - Если этот флажок установлен, то сервер будет сканировать удаленные компьютеры, используя протокол SMB, без установки агента на удаленную систему. В зависимости от заданных правил обнаружения контента может потребоваться полная проверка содержимого файлов. В этом случае проверяемые файлы передаются на сервер для проведения анализа, что может повлечь повышенную нагрузку на сеть и снизить её пропускную способность.
- **Автоматически устанавливать агент Discovery** - Если этот флажок установлен, то агент сервера Discovery будет автоматически установлен на удаленную систему при условии, что он не был установлен ранее, а на удаленной системе не запущен Cyber Protego Agent со встроенным агентом сервера Discovery.
- **Автоматически удалять агент Discovery** - Если этот флажок установлен, то агент сервера Discovery будет автоматически удален с удаленной системы по завершении сканирования. Обратите внимание, что этот параметр не приводит к удалению Cyber Protego Agent со встроенным агентом сервера Discovery.

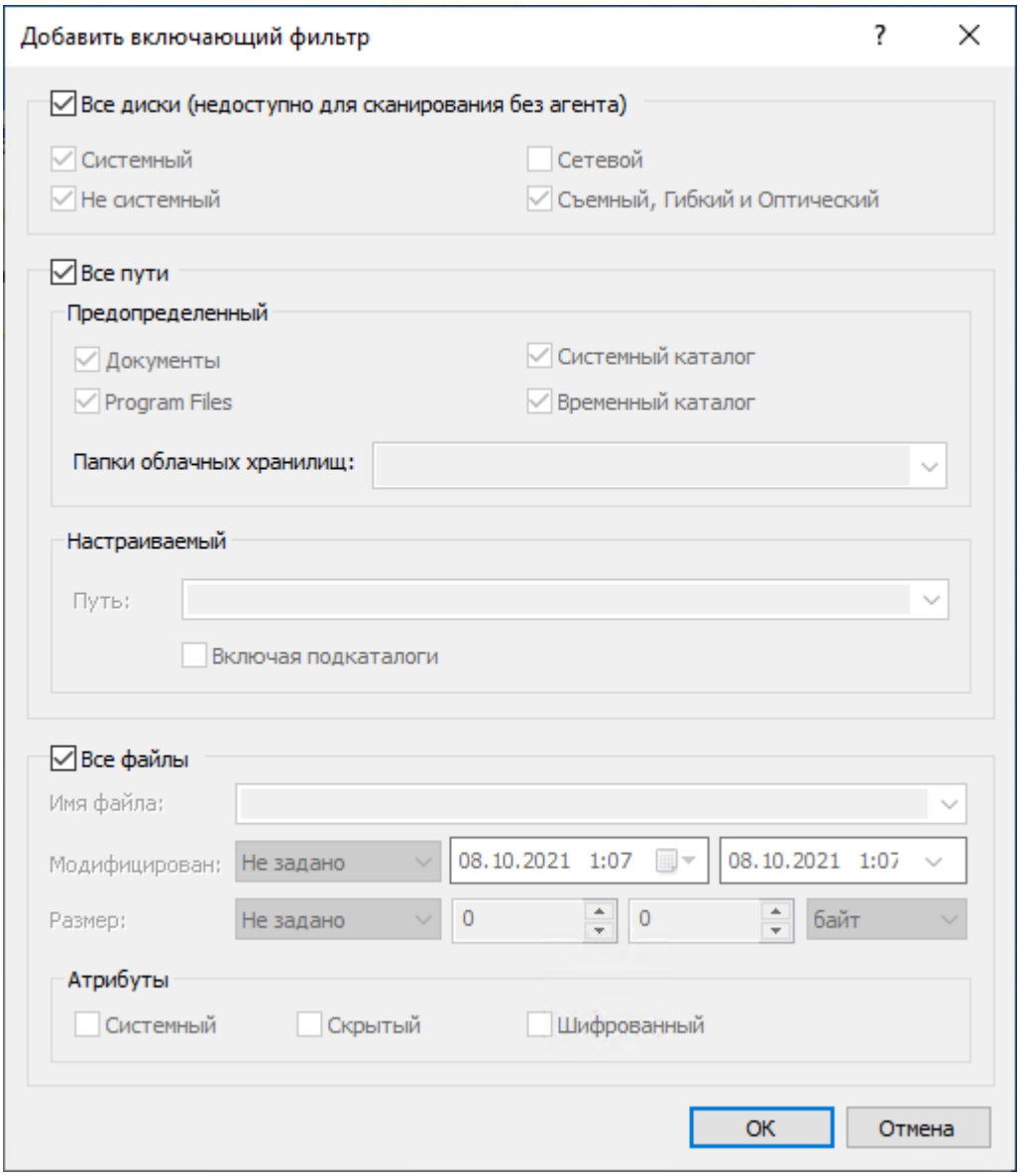
Примечание
Если служба Search and Discovery Server запускается под локальной учетной записью системы (Local System), то Сервер Discovery не может устанавливать или удалять агенты Discovery на удаленных компьютерах.

Созданное подразделение будет отображено в дереве консоли.

Добавление фильтров

Ниже описывается настройка фильтров для подразделения компьютеров. О настройке фильтров для подразделения Elasticsearch см. в разделе Диалоговое окно управления фильтром для Elasticsearch.

В зависимости от типа добавляемого фильтра (включающий или исключающий), для настройки фильтра используется диалоговое окно **Добавить включающий фильтр** или **Добавить исключающий фильтр**.



Заполните это диалоговое окно следующим образом.

1. Укажите диски, которые следует включить или исключить в процессе сканирования:
   - **Все диски** - Задайте типы дисков для сканирования. Данные параметры не поддерживаются в режиме сканирования без агента, при котором сканируются все диски независимо от их типа.

     Примечание
     Если флажок **Все диски** установлен, то описанные ниже флажки не действуют, и фильтр будет включать или исключать все диски.

     - **Системный** - Задать сканирование системного логического диска, на котором установлена операционная система Windows.
     - **Не системный** - Задать сканирование всех остальных логических и физических дисков, не подпадающих под определение системного диска.

- **Сетевой** - Задать сканирование подключенных сетевых дисков. Многие сетевые диски могут быть доступны для каждого из пользователей компьютера. Сканированию подвергаются все сетевые диски для всех пользователей.
- **Съемный, Гибкий и Оптический** - Задать сканирование съемных носителей, таких как флоппи-диски, оптические накопители (CD/DVD/BD-ROM), вставленные в компьютеры карты памяти, подключенные через USB внешние устройства хранения данных и т. п.

2. Укажите пути, которые следует включить или исключить в процессе сканирования:
   - **Все пути** - Задайте папки для сканирования на дисках.

     Примечание
     Если флажок **Все пути** установлен, то описанные ниже флажки не действуют, и фильтр будет включать или исключать все папки.

     - **Документы** - Задать пользовательскую папку Документы. Это папка %SystemDrive%\Users\<user>\Documents. Сканируются папки документов для каждого пользователя.
     - **Program Files** - Задать папку Program Files. На 64-битных системах сканируются папки Program Files и Program Files (x86).
     - **Системный каталог** - Задать системную папку Windows.
     - **Временный каталог** - Задать системную папку временных файлов.
     - **Папки облачных хранилищ** - Задать сканирование локальных папок синхронизации облачных агентов файлового обмена. Поддерживаются следующие агенты: Amazon Cloud Drive, Box, Облако Mail.Ru, Copy, Dropbox, Google Drive, iCloud, MediaFire, OneDrive, SpiderOak, SugarSync, Яндекс.Диск.

     Примечание
     Сканирование папки агента **Box** возможно только когда пользователь (владелец локальной папки синхронизации) выполнил вход в систему.

   - **Путь** - Задать пути для сканирования вручную. Можно ввести несколько через запятую (,) или точку с запятой (;). Поддерживаются пути в формате UNC (например, \\server\share). Допускается использование знаков подстановки, таких как звездочка (*) и вопросительный знак (?).
     См. также Сканирование сетевого ресурса: Пример.
   - **Включая подкаталоги** - Задать условие для сканирования вложенных папок. Если этот флажок установлен, сканируются файлы, находящиеся как в заданных папках, так и во вложенных папках.
3. Укажите файлы, которые следует включить или исключить в процессе сканирования:
   - **Все файлы** - Задайте файлы для сканирования на дисках.

     Примечание
     Если флажок **Все файлы** установлен, то описанные ниже флажки не действуют, и фильтр будет включать или исключать все файлы.

- **Имя файла** - Задать имена файлов для сканирования. Различные имена файлов разделяются точкой с запятой (;), например, *.doc; *.docx.
  Допускается использование знаков подстановки, таких как звездочка (*) и вопросительный знак (?). Звездочка обозначает произвольный ряд символов или их отсутствие. Например, *.txt соответствует любому имени файла с расширением txt. Вопросительный знак обозначает один произвольный символ. Например, ????.* соответствует имени из любых 4-х символов с любым расширением.
- **Модифицирован** - Задать дату/время последнего изменения файла. Для этого следует выбрать соответствующую опцию в раскрывающемся списке поля **Модифицирован**:
  - **Не задано** (выбор по умолчанию).
  - **До** - Дата/время последнего изменения файла должна быть ранее указанной.
  - **После** - Дата/время последнего изменения файла должна быть позднее указанной.
  - **Между** - Дата/время последнего изменения файла должна быть в пределах указанного промежутка.
  - **Не старше чем** - После даты/времени последнего изменения файла должно пройти не более указанного числа секунд, минут, часов, дней, недель, месяцев или лет.
  - **Старше чем** - После даты/времени последнего изменения файла должно пройти не менее указанного числа секунд, минут, часов, дней, недель, месяцев или лет.
- **Размер** - Задать размер файла в байтах, килобайтах, мегабайтах, гигабайтах или терабайтах. Для этого следует выбрать соответствующую опцию в раскрывающемся списке поля **Размер**:
  - **Не задано** (выбор по умолчанию).
  - **Равно** - Размер файла должен быть равен заданному.
  - **Меньше чем** - Размер файла должен быть менее заданного.
  - **Больше чем** - Размер файла должен быть более заданного.
  - **Между** - Размер файла должен быть в заданном интервале значений.
- **Атрибуты** - Задать атрибуты файла. Используемые атрибуты **Системный**, **Скрытый** и **Шифрованный** соответствуют аналогичным атрибутам файловой системы NTFS.

Создание фильтра: Пример

Данный пример описывает настройку фильтров для сканирования любых съемных носителей (в т.ч. подключенных USB-дисков), а также папки D:\Custom\.

Чтобы создать подразделение с такой областью поиска, должны быть заданы два включающих фильтра. Один, задающий сканирование всех типов съемных носителей, и второй, задающий сканирование указанной папки. Следует отметить, что, если создать один фильтр с сочетанием обеих описанных областей сканирования, будет применен логический оператор И, так что созданный фильтр будет ограничивать область сканирования папкой D:\Custom\ на съемных носителях.

Создайте первый включающий фильтр для сканирования любых съемных носителей:

- Снимите флажок **Все диски**, а также все остальные флажки в данной категории. Установите флажок **Съемный, Гибкий и Оптический**.
- Установите флажок **Все пути**.
- Установите флажок **Все файлы**.

Создайте второй включающий фильтр для сканирования папки D:\Custom\:

- Установите флажок **Все диски**.
- Снимите флажок **Все пути**, а также все остальные флажки в данной категории. Введите D:\Custom\ в поле **Путь** в категории **Настраиваемый**.
- Установите флажок **Все файлы**.

Сканирование сетевого ресурса: Пример

Предположим, что требуется сканировать сетевой ресурс на сервере или NAS-устройстве с операционной системой, на которой Cyber Protego не может быть установлен (например, ОС Linux). Сетевой ресурс идентифицируется по пути UNC (например, \\server\share).

Такое сканирование можно выполнить, настроив подразделение следующим образом:

- В подразделение добавьте компьютер, с которого можно получить доступ к сетевому ресурсу. Это может быть компьютер, на котором работает Сервер Discovery, или другой компьютер, операционная система которого допускает установку Cyber Protego (например, ОС Windows). Инструкции см. в разделе Создание подразделения.
- Убедитесь, что учетная запись пользователя, под которой Сервер Discovery сканирует данный компьютер, имеет достаточные права доступа к сетевому ресурсу. Требуется как минимум доступ на чтение. Если в процессе сканирования Сервер Discovery должен будет вносить изменения на сетевом ресурсе (например, выполнять шифрование файлов или установку разрешений), потребуются соответствующие права доступа.
  Если учетная запись пользователя, используемая по умолчанию для выполнения сканирования, не имеет достаточных прав доступа к сетевому ресурсу, настройте подразделение на использование альтернативных параметров доступа. В диалоговом окне для создания или редактирования подразделения нажмите кнопку **Установить параметры доступа** и укажите имя и пароль пользователя, обладающего требуемыми правами доступа.
- В подразделение добавьте включающий фильтр, у которого в поле **Путь** укажите UNC-путь сетевого ресурса.

Настройте правила обнаружения контента (см. раздел Правила и действия), создайте задачу обнаружения на основе настроенного подразделения и правил (см. раздел Задачи), и затем запустите эту задачу для выполнения требуемого сканирования.

Управление подразделениями

Подразделения отображаются в дереве консоли под узлом **Search and Discovery Server** > **Сервер Discovery** > **Подразделения**.

Если в дереве консоли выбрано подразделение, на панели сведений отображается содержимое этого подразделения:

По каждому компьютеру из выбранного подразделения на панели сведений предоставляется следующая информация:

- **Имя объекта** - Имя, идентифицирующее компьютер.
- **Статус** - Текущий статус компьютера. Может иметь одно из следующих значений:
  - **Ожидает** - Компьютер находится в режиме ожидания запуска задачи сканирования. Данный статус назначается, когда соответствующая задача получает статус **Выполняется**.
  - **Сканирование** - Компьютер сканируется в настоящий момент.
  - **Закончено** - Задача сканирования для данного компьютера успешно завершена.
  - **Истекло** - Во время выполнения задачи сканирования компьютер стал недоступен (например, компьютер отключился от сети, изменились сетевые настройки, или какая-либо иная проблема не позволила агенту Discovery передать данные на сервер) и не отвечал в течение всего времени, определенного параметром Время ожидания агента.
    Статус **Истекло** также назначается, если задача сканирования занимает больше времени, чем задано параметром Остановить, если выполняется дольше, что приводит к преждевременному принудительному завершению задачи.
  - **Доступ запрещен** - Возникла проблема с доступом к данному ресурсу (компьютеру). Это может означать, что данные учетной записи, заданные для данного подразделения, не могут быть использованы (ошибка сертификата или данных стартовой учетной записи в зависимости от конфигурации).
  - **Ошибка установки** - При установке агента Discovery на данный компьютер возникла проблема.
  - **Лицензия недоступна** - Недостаточно лицензий для сканирования данного компьютера.
  - **Отменяется** - Задача сканирования отменяется в настоящий момент.
  - **Отменено** - Задача сканирования была отменена.
  - **Компьютер недоступен** - После числа попыток, определенного параметром Кол-во попыток, или по истечении времени, определенного параметром Таймаут попыток, произошла одна из следующих проблем:
    - Неуспешная попытка подключения к удаленному компьютеру для запуска сканирования (в режиме сканирования без агента)
    - Неуспешная попытка подключения к удаленному компьютеру и ассоциирования задачи сканирования с агентом Discovery. Такая проблема проявляется, когда компьютер становится недоступным (выключен либо не подсоединен к сети), либо агент Discovery не был установлен или запущен на данном компьютере при том, что автоматическая установка агента не задана в свойствах данного подразделения (не установлен флаг **Автоматически устанавливать агент Discovery**).
- **Просканировано объектов** - Общее число сканированных объектов. Значение в скобках указывает количество сканированных вложенных объектов.

Пример: “1 (20)” означает 1 контейнер (архив) с 20 файлами внутри.

Для каждого подразделения в списке подсчитывается и отображается общее количество объектов, прошедших проверку при последнем сканировании данного подразделения. Счетчик сканированных объектов подразделения сбрасывается при каждом очередном запуске сканирования этого подразделения. Это же относится и к другим счетчикам.

Для подразделений Elasticsearch объектом сканирования является поле документа, а не сам документ. У каждого такого подразделения подсчитывается и отображается общее количество полей, прошедших проверку при сканировании данного подразделения.

- **Запущен** - Дата и время начала сканирования данного подразделения сервером.
- **Закончен** - Дата и время завершения сканирования данного подразделения сервером.
- **Сработало правил** - Число различных правил обнаружения, успешно сработавших при сканировании контента. Если некоторое правило сработало более одного раза, значение счетчика не увеличится.
- **Выполнено действий** - Число действий, выполненных в ходе сканирования.
  Пример: Если в результате срабатывания правила был удален файл, запротоколировано событие и отправлено уведомление, то значение данного счетчика увеличится на 3.
- **Предупреждения** - Число ошибок сканирования. Данный счетчик увеличивается, если был обнаружен объект, соответствующий условиям правила обнаружения, но для него не удалось выполнить заданное действие, либо не удалось выполнить контентный анализ (например, при попытке сканировать зашифрованный или поврежденный архив).

Контекстное меню подразделения в дереве консоли содержит следующие команды:

- **Редактировать подразделение** - Просмотреть или изменить параметры подразделения в диалоговом окне, которое открывает эта команда.
- **Дублировать подразделение** - Создать новое подразделение путем копирования параметров выбранного подразделения. Параметры нового подразделения можно редактировать в диалоговом окне, которое открывает эта команда.
  Имя нового подразделения по умолчанию состоит из префикса **Копия**, за которым следует имя выбранного подразделения. При создании двух или более копий к новому имени по умолчанию добавляется числовой суффикс, указывающий номер копии.
- **Редактировать список компьютеров** - Просмотреть или изменить список компьютеров, входящих в состав данного подразделения. Список компьютеров можно редактировать в диалоговом окне, которое открывает эта команда.
- **Удалить подразделение** - Удалить выбранное подразделение.
- **Обновить** - Обновить список на панели сведений с учетом последних изменений.
  Поскольку информация на панели сведений не обновляется автоматически, для ее обновления служит команда **Обновить**.

Управление компьютерами подразделения выполняется посредством контекстного меню. Чтобы открыть меню, выполните следующие действия:

1. В дереве Центральной консоли управления раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Подразделения**.

2. В списке подразделений под узлом **Подразделения** выберите требуемое подразделение.
   В правой панели откроется список компьютеров подразделения.
3. Щелкните правой кнопкой мыши на требуемом компьютере.
   Появится контекстное меню.

Контекстное меню компьютера на панели сведений включает все команды контекстного меню подразделения, а также содержит команды для данного компьютера:

- **Открыть ошибки в просмотрщике журнала** - Открыть просмотрщик журнала задач с предопределенным фильтром, заданным для просмотра только ошибок сканирования для выбранного компьютера. Будут отображены все ошибки, случившиеся во всех задачах в течение определенного периода времени.
- **Открыть предупреждения в просмотрщике журнала** - Открыть просмотрщик журнала задач с предопределенным фильтром, заданным для просмотра только информационных предупреждений сканирования для выбранного компьютера. Будут отображены все предупреждения, выданные во всех задачах в течение определенного периода времени.

Подразделения Elasticsearch

Cyber Protego Discovery дает возможность эффективно обнаруживать интересующие документы в Elasticsearch - распределенной программной системе, обеспечивающей индексирование и поиск различных типов данных в реальном времени. Сервер Discovery запрашивает поиск документов по заданным параметрам, а затем применяет правила и действия обнаружения к полученным от Elastcicsearch документам. На соответствие правилам проверяются данные полей документа, определенных настройками фильтра (см. Диалоговое окно управления фильтром для Elasticsearch). Правило срабатывает, если ему соответствуют данные хотя бы одного такого поля.

Внимание

- Cyber Protego Discovery обеспечивает обнаружение документов в Elasticsearch версии 6.8.12 или более новой.
- Для обнаружения документов в Elasticsearch требуется по одной лицензии Cyber Protego Discovery на каждый индекс Elasticsearch, в котором необходимо выполнить поиск.
- Cyber Protego Agent Discovery на узлах Elasticsearch не устанавливается. Обнаружение выполняется без использования агента.
- Действия обнаружения в отношении Elasticsearch ограничиваются протоколированием событий и отправкой алертов. Сервер Discovery не может изменять и удалять документы в Elasticsearch.

Для работы с Elasticsearch в задаче обнаружения необходимо использовать подразделение специального типа: при его создании выберите пункт **Узлы Elasticsearch** в списке **Тип подразделения**. Для настройки подразделений данного типа используются следующие параметры:

- **Серверы** - Настраиваемый список компьютеров, на которых работают подлежащие обнаружению узлы Elasticsearch. Нажмите кнопку **Редактировать** рядом с полем **Серверы**. В появившемся диалоговом окне можно просматривать текущий список, добавлять имена

компьютеров в список и удалять их из списка.
Имена компьютеров, на которых работают требуемые узлы Elasticsearch, перечисляются в правой части диалогового окна. Для добавления компьютеров в список, введите их имена или IP-адреса в левой части окна и нажмите кнопку > . В качестве имени компьютера можно ввести имя хоста или полностью определенное имя домена (FQDN). После ввода каждого имени нажимайте ENTER. Для удаления компьютеров из списка выберите их имена в левой части окна и нажмите кнопку < .

При вводе имени компьютера можно указать номер сетевого порта, используемого Elasticsearch, в формате имя:порт. Если порт не указан, задача обнаружения будет сканировать все порты, пока не обнаружит Elasticsearch. Чтобы ускорить сканирование портов, можно установить флажок **Умный поиск портов**. Если этот флажок установлен, задача обнаружения будет сканировать только те порты, которые обычно используются серверами Elasticsearch. Поскольку поиск порта может занимать много времени, желательно явно указывать номер порта, используемого Elasticsearch.

- **Установить параметры доступа** - Нажмите эту кнопку, чтобы указать имя и пароль учетной записи с достаточными правами для доступа к узлам Elasticsearch на серверах, входящих в данное подразделение. Имя и пароль необходимо указать, если Elasticsearch требует авторизованного доступа. Если имя и пароль учетной записи не указаны, Сервер Discovery использует анонимный доступ к Elasticsearch.

Примечание
При использовании базы данных другого сервера Discovery потребуется заново ввести имя и пароль учетной записи. Поскольку эти параметры зашифрованы защищенным ключом, хранящемся на данном сервере Discovery, они не могут быть расшифрованы другим сервером, так что имя и пароль необходимо ввести заново.

- **Включающие фильтры** - Условия включения индексов и документов в процесс обнаружения. Поиск ведется только по индексам и документам, которые соответствуют хотя бы одному из таких фильтров. Кнопки под этим полем позволяют добавлять, редактировать и удалять включающие фильтры. При добавлении и редактировании фильтра используется Диалоговое окно управления фильтром для Elasticsearch.
- **Исключающие фильтры** - Условия исключения индексов и документов из процесса обнаружения. Поиск не ведется по индексам и документам, которые соответствуют любому из таких фильтров. Кнопки под этим полем позволяют добавлять, редактировать и удалять исключающие фильтры. При добавлении и редактировании фильтра используется Диалоговое окно управления фильтром для Elasticsearch.
- **Запрашивать** <число> **документов** - Установите этот флажок, чтобы задать максимальное количество документов, запрашиваемых у Elasticsearch. В процессе обнаружения Elasticsearch возвратит не более указанного количества документов, которые соответствуют заданным фильтрам. Снимите этот флажок, если требуется, чтобы Elasticsearch возвращал все соответствующие фильтрам документы.
- **Сортировка** - Порядок сортировки документов, возвращаемых Elasticsearch. Снимите флажок **Сортировать**, если не важно, в каком порядке поступают документы от Elasticsearch

(сортировка по умолчанию). Установите этот флажок, чтобы документы поступали в порядке возрастания или убывания значений некоторого поля документа. Укажите имя этого поля в параметре **По полю** и выберите нужный порядок сортировки (**возрастание** или **убывание**).

Примечание
Одно и то же поле можно индексировать по-разному для разных целей (так называемое поле *multi-field*). Например, поле типа string может описываться в индексе как поле типа text для полнотекстового поиска и как поле типа keyword для сортировки и агрегирования. В таком случае поле для сортировки желательно указывать в виде имя_поля.keyword.

Для каждого фильтра отображаются следующие условия:

- **Индекс** - Список имен индексов. Фильтру соответствуют документы любого из перечисленных индексов.
  В именах индексов могут использоваться знаки подстановки: звездочка (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа. Например, точка со звездочкой (.*) обозначает любой индекс, имя которого начинается с точки.
  Условие <Все> означает, что фильтру соответствуют документы из любого индекса.
- **Поле : Значение / Запрос** - Список пар “поле-значение” или поисковый запрос. Здесь “Поле” - это имя поля в документах Elasticsearch, а “Значение” - это искомое значение указанного поля. “Запрос” - это строка запроса в соответствии с синтаксисом поисковых запросов Elasticsearch. Если задан список пар “поле-значение”, фильтру соответствуют документы, у которых указанные поля имеют указанные значения. Если задана строка запроса, фильтру соответствуют документы, возвращаемые соответствующим поисковым запросом.
  Отметка <Все значения> в паре “поле-значение” указывает, что фильтру соответствуют документы с любым значением данного поля.
  Отметка <Все> означает, что фильтру соответствуют любые документы из указанных индексов.

Имена индексов, начинающиеся с точки, обычно обозначают системные индексы (например, .kibana). Поскольку такие индексы содержат параметры конфигурации и другие системные данные, желательно исключить их из процесса обнаружения. Поэтому для исключающего фильтра по умолчанию установлены следующие значения параметров: Индекс = .*; Поле : Значение / Запрос = Все, что исключает все документы во всех индексах, имена которых начинаются с точки.

Диалоговое окно управления фильтром для Elasticsearch

Фильтр позволяет задать параметры поиска документов в Elasticsearch и определяет поля документа, подлежащие обнаружению. Правила обнаружения применяются к индексам и документам, которые соответствуют включающему фильтру и не соответствуют исключающему фильтру. На соответствие правилам проверяются поля, заданные настройками включающего фильтра (подробнее см. в разделе Поля).

Диалоговое окно управления фильтром используется при добавлении и редактировании фильтра. В нем предоставляются следующие элементы управления условиями фильтра:

- Индексы - Фильтрация по местоположению документа.
- Поля - Фильтрация по данным полей документа.

Индексы

Установите флажок **Все индексы**, если требуется, чтобы фильтру соответствовали документы из любого индекса. Снимите этот флажок, если требуется явно указать индексы. В результате фильтру будут соответствовать только документы из индексов, имена которых перечислены в поле **Индекс**.

В поле **Индекс** можно ввести несколько имен через точку с запятой (;), а также использовать знаки подстановки: звездочку (*) для обозначения произвольной последовательности символов, вопросительный знак (?) для обозначения любого одиночного символа.

Для облегчения настройки фильтров поле **Индекс** запоминает ранее введенные имена и позволяет выбирать их из раскрывающегося списка.

Поля

Установите флажок **Все документы**, если требуется, чтобы фильтру соответствовали любые документы из указанных индексов. Снимите этот флажок, если требуется отфильтровать документы по значениям их полей или использовать поисковый запрос. В результате фильтру будут соответствовать только документы, соответствующие каждой из указанных пар “поле-значение” (опция **Настраиваемый**), или документы, возвращаемые указанным поисковым запросом Elasticsearch (опция **Запрос**).

Включающий фильтр определяет также, какие поля документа будут проверяться правилами обнаружения. Если у такого фильтра выбрана опция **Настраиваемый**, будут проверяться только поля, указанные в парах “поле-значение” фильтра. Если установлен флажок **Все документы** или выбрана опция **Запрос**, будут проверяться все поля документа. Выбор полей для проверки определяется только включающим фильтром. Исключающий фильтр позволяет исключать документы, но не поля для проверки.

Внимание
В пределах одного фильтра пары “поле-значение” объединяются по И, так что фильтру соответствуют документы, соответствующие каждой из указанных пар. Фильтры подразделения объединяются по ИЛИ, так что включаются/исключаются документы, которые соответствуют хотя бы одному из заданных в подразделении фильтров.

Чтобы задать список пар “поле-значение”, выберите опцию **Настраиваемый**. Щелкните в первом столбце списка, чтобы ввести имя поля. Чтобы ввести искомое значение, щелкните во втором столбце рядом с именем поля. Фильтру соответствуют документы, у которых указанные поля имеют указанные значения.

Если указано только значение поля, фильтру соответствуют документы с данным значением в любом поле. В качестве имени поля для такого значения в списке отображается отметка <Все>. Таким образом можно отбирать документы по определенному значению независимо от поля, в котором встречается это значение.

Если указано только имя поля, фильтру соответствуют документы с любым значением данного поля. В качестве значения для такого поля в списке отображается отметка <Все значения>. Таким образом можно задать искомые поля документов и применить правила обнаружения к данным, которые содержатся в этих полях.

Если указано и поле, и значение, при выполнении задачи обнаружения пара “поле-значение” будет преобразована в строку запроса на поиск в Elasticsearch. Фильтру будут соответствовать только документы, возвращаемые этим запросом. Указанное для поля значение должно иметь синтаксис, поддерживаемый в строке запроса Elasticsearch.

Поисковый запрос можно также задать явным образом. Для этого выберите опцию **Query** (Запрос). Затем введите строку запроса в соответствии с синтаксисом поисковых запросов Elasticsearch (см. www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-query.html#query-string-syntax). Таким образом можно задавать область обнаружения при помощи поисковых запросов. Например, строка запроса author:"John Smith" AND title:(quick OR brown) порождает запрос на поиск документов, у которых в поле author содержится строка John Smith, а в поле title содержится слово quick или слово brown.

Правила и действия

Правила обнаружения определяют тип контента, который должен быть обнаружен, а также задают действия, которые следует выполнить над обнаруженными данными. Подобно контентно-зависимым правилам Cyber Protego Agent, эти правила используют контентные группы для определения данных, к которым применимо то или иное правило.

Правила обнаружения создаются на основе контентных групп, позволяющих централизованно определять типы контента для обнаружения. В каждом правиле используется определенная контентная группа и указываются действия, применяемые к обнаруженным данным. Контентная группа правила задает критерии поиска данных, к которым будут применяться эти действия.

Все контентные группы содержатся в базе данных контента, хранимой в базе данных сервера Discovery. Соответственно, все консоли, взаимодействующие с сервером, оперируют одним экземпляром базы данных контента.

Примечание
Контентные группы из базы данных контента Cyber Protego Agent могут быть импортированы в Сервер Discovery. Инструкции см. в разделе Импорт и экспорт правил.

Предусмотрены следующие типы контентных групп:

- **Определение типа файла** - Выявление файлов по сигнатурам файловых типов.
- **Ключевые слова** - Поиск определенных ключевых слов или фраз в файлах/данных.
- **Шаблон** - Поиск фрагментов текста по определенным шаблонам, описываемых регулярными выражениями Perl.
- **Свойства документа** - Поиск файлов-документов с определенными свойствами (например, имя документа, его размер и т. п.).

- **Цифровые отпечатки** - Проверка цифровых отпечатков файлов или данных.
- **Составное** - Построение логического выражения из групп различных типов.

Узел “Правила и действия”

При выборе узла **Search and Discovery Server** > **Сервер Discovery** > **Правила и действия** в дереве консоли, на панели сведений появляется список всех правил обнаружения контента, которые в данный момент существуют на сервере.

По каждому правилу отображаются следующие сведения:

- **Имя** - Имя правила. По умолчанию имя правила совпадает с именем его контентной группы.
- **Тип** - Тип анализа контента файла. Возможные значения:
  - **Определение типа файла** - Идентификация файлов ведется по сигнатурам.
  - **Ключевые слова** - Идентификация данных/файлов ведется по заданным ключевым словам и выражениям.
  - **Шаблон** - Идентификация данных/файлов ведется на основе заданных шаблонов регулярных выражений Perl.
  - **Свойства документа** - Идентификация файлов ведется по их свойствам.
  - **Цифровые отпечатки** - Идентификация файлов/данных ведется по их цифровым отпечаткам.
  - **Составное** - Идентификация данных/файлов ведется по заданному контенту, описанному логическим выражением.
- **Применяется к** - Тип подразделений, для которых данное правило может использоваться в задачах обнаружения. Возможна любая комбинация следующих значений:
  - **Компьютеры** - Правило может использоваться для обнаружения файлов на компьютерах или серверах.
  - **Узлы Elasticsearch** - Правило может использоваться для обнаружения документов в Elasticsearch.
- **Действие** - Указывает действие данного правила в отношении обнаруженного контента. Возможны следующие действия:
  - **Удалить** - Удаление обнаруженного контента.
  - **Безопасное удаление** - Удаление обнаруженного контента с использованием безопасной процедуры уничтожения данных по стандарту US DoD 5220.22-M.
  - **Шифровать** - Шифрование обнаруженного контента с помощью технологии Windows EFS (Encrypted File System).
  - **Установить разрешения** - Настройка определенные разрешения файловой системы для обнаруженных файлов.
  - **Применять к контейнерам** - Действие применяется также к файлам архивов (например, файлам ZIP или RAR), которые содержат обнаруженный контент.
  - **Протоколировать** - Запись информации об обнаруженном контенте в журнал задач сервера Discovery.

- **Отправить алерт** - Отправка тревожного алерта об обнаруженном контенте.
- **Оповестить пользователя** - алерт текущего пользователя посредством системного уведомления (отображается в области уведомлений панели задач Windows).

Контекстное меню узла **Правила и действия** содержит следующие команды:

- **Управление** - Открыть диалоговое окно, предоставляющее возможность создавать, просматривать, изменять или удалять правила обнаружения контента и контентные группы.
- **Загрузить** - Импортировать правила из файла. Эта команда позволяет импортировать как правила обнаружения контента сервера Discovery, так и контентно-зависимые правила и контентные группы Cyber Protego Agent.
- **Сохранить** - Экспортировать все правила в файл.
  Правила можно экспортировать в файл и затем импортировать их из этого файла. Эта возможность может быть полезной, например, при необходимости скопировать правила на другой сервер.
- **Обновить** - Обновляет список на панели сведений с учетом последних изменений.
  Поскольку информация на панели сведений не обновляется автоматически, для ее обновления служит команда **Обновить**.

Контекстное меню правила на панели сведений содержит следующие команды:

- **Управление** - Открыть диалоговое окно, предоставляющее возможность создавать, просматривать, изменять или удалять правила обнаружения контента и контентные группы.
- **Редактирование правила** - Открыть диалоговое окно, предоставляющее возможность просмотреть или изменить действие правила, а также переименовать правило.
- **Дублировать правило** - Создать новое правило путем копирования параметров выбранного правила. Имя и действие нового правила можно изменить в диалоговом окне, которое открывает эта команда.
  Имя нового правила по умолчанию состоит из префикса **Копия**, за которым следует имя выбранного правила. При создании двух или более копий к новому имени по умолчанию добавляется числовой суффикс, указывающий номер копии.
- **Удалить правило** - Удалить выбранное правило.
- **Обновить** - Обновляет список на панели сведений с учетом последних изменений.
  Поскольку информация на панели сведений не обновляется автоматически, для ее обновления служит команда **Обновить**.

Определение и изменение правил и действий

Правила обнаружения контента определяются и изменяются в диалоговом окне **Правила и действия**.

Чтобы создать правило обнаружения контента

1. Откройте консоль управления Cyber Protego Центральная консоль управления.
2. В дереве консоли раскройте узлы **Search and Discovery Server** > **Сервер Discovery**.

3. В узле **Сервер Discovery** выполните одно из следующих действий.
   - Щелкните правой кнопкой мыши **Правила и действия**, затем выберите команду **Управление**.
     - или -
   - Выберите **Правила и действия**, затем щелкните по значку **Управление** на панели инструментов.

Настройка правил обнаружения контента в Cyber Protego Discovery аналогична настройке контентно-зависимых правил в Cyber Protego Content Control.

Чтобы изменить, дублировать или удалить правило обнаружения контента

1. Откройте консоль управления Cyber Protego Центральная консоль управления.
2. В дереве консоли раскройте узлы **Search and Discovery Server** > **Сервер Discovery**.
3. В узле **Сервер Discovery** выберите **Правила и действия**.
4. На панели сведений щелкните правой кнопкой по правилу, которое нужно изменить, дублировать или удалить, а затем выберите команду в открывшемся контекстном меню.

Использование диалогового окна “Правила и действия”

Для создания и редактирования правил обнаружения контента служит диалоговое окно **Правила и действия**. Это окно можно открыть, выбрав команду **Управление** из контекстного меню узла **Правила и действия** в дереве консоли. Диалоговое окно **Правила и действия** предоставляет средства управления контентными группами и правилами обнаружения контента в сервере Discovery.

Правила обнаружения контента создаются на основе контентных групп, которые позволяют централизованно определять типы контента для обнаружения. Можно использовать встроенные контентные группы, создавать их редактируемые копии (дубликаты) или создавать собственные контентные группы, необходимые для решения частных задач организации.

Чтобы просмотреть контентную группу

- В верхней части диалогового окна в области **База данных контента** выберите контентную группу, а затем нажмите кнопку **Просмотр группы**.

Встроенные контентные группы невозможно изменять, но можно создавать и редактировать их копии, необходимые для решения частных задач организации.

Чтобы создать копию контентной группы

1. В верхней части диалогового окна в области **База данных контента** выберите контентную группу, а затем нажмите кнопку **Дублировать**.
2. В появившемся диалоговом окне внесите необходимые изменения в группу, а затем нажмите кнопку **OK**. Новая контентная группа добавляется в список существующих контентных групп в области **База данных контента** в верхней части диалогового окна **Правила и действия**.

Пользовательские контентные группы можно изменять или удалять в любое время.

Чтобы изменить или удалить пользовательскую контентную группу

1. В верхней части диалогового окна в области **База данных контента** выберите пользовательскую контентную группу.
2. Чтобы изменить выбранную группу, нажмите кнопку **Редактировать группу**. В появившемся диалоговом окне внесите необходимые изменения, а затем нажмите кнопку **OK**.

   - или -

   Чтобы удалить выбранную группу, нажмите кнопку **Удалить группу** или клавишу DELETE.
3. В диалоговом окне **Правила и действия** нажмите кнопку **OK** или **Применить**, чтобы сохранить изменения.

Можно протестировать встроенные и пользовательские контентные группы, чтобы посмотреть, попадают ли под них заданные файлы. Используя эти тесты, можно убедиться, что контентно-зависимые правила, созданные на основе контентных групп, соответствуют поставленным бизнес-задачам.

Чтобы протестировать контентную группу

1. В верхней части диалогового окна в области **База данных контента** выберите любую контентную группу, которую необходимо протестировать, а затем нажмите кнопку **Тестировать группу**. За один раз можно протестировать только одну контентную группу.
2. В появившемся диалоговом окне выберите и откройте файл, который будет использован для тестирования контентной группы.
   Консоль отобразит окно сообщения **Результат**. Если тестовый файл попадает под указанную контентную группу, окно сообщения будет содержать следующий текст: “Выбранный файл совпадает с группой”. Если тестовый файл не соответствует указанной контентной группе, окно сообщения будет содержать следующий текст: “Выбранный файл не совпадает с группой”.

   Примечание
   Во время тестирования консоль может перестать отвечать (“зависает”)

Правила обнаружения контента создаются на основе встроенных или пользовательских контентных групп.

Чтобы создать правило обнаружения контента

1. В верхней части диалогового окна **Правила и действия** в области **База данных контента** выберите требуемую контентную группу, а затем нажмите кнопку Добавить.

   Примечание
   Для каждого создаваемого правила можно указать только одну контентную группу.

2. В диалоговом окне **Добавить правило** задайте свойства правила, а затем нажмите кнопку **OK**. Созданное правило отображается в области **Правила и действия** в нижней части диалогового окна **Правила и действия**.
3. Нажмите кнопку **OK** или **Применить**, чтобы сохранить правило.

Можно редактировать свойства правил, такие как **Имя** и **Действие**.

Чтобы редактировать правило обнаружения контента

1. В нижней части диалогового окна в области **Правила и действия** выберите правило, а затем нажмите кнопку **Редактировать**.

   - или -

   Щёлкните правило правой кнопкой мыши и выберите команду **Редактировать**.
2. В появившемся диалоговом окне **Редактирование правила** внесите необходимые изменения.
3. Нажмите кнопку **OK**, чтобы сохранить изменения.

Заданные правила возможно сохранить (экспортировать) в файле формата .dra, который затем можно загрузить (импортировать) и использовать на другом компьютере. Кроме того, предусмотрена возможность импортировать правила обнаружения контента из файла с контентно-зависимыми правилами Cyber Protego Agent в формате .cwl. Экспорт и импорт правил могут быть также использованы как вариант резервного копирования.

Чтобы экспортировать правила обнаружения контента

1. В нижней части диалогового окна в области **Правила и действия** нажмите кнопку **Сохранить**.
2. В появившемся диалоговом окне укажите файл для хранения экспортированных правил. При экспорте правила сохраняются в файле с расширением .dra.

Чтобы импортировать правила обнаружения контента или контентно-зависимые правила

1. В нижней части диалогового окна в области **Правила и действия** нажмите кнопку **Загрузить**.
2. В появившемся диалоговом окне найдите и откройте файл, в котором хранятся ранее экспортированные правила.
   За один раз можно импортировать только один файл .dra или .cwl.

Можно удалять правила обнаружения контента, если они больше не нужны.

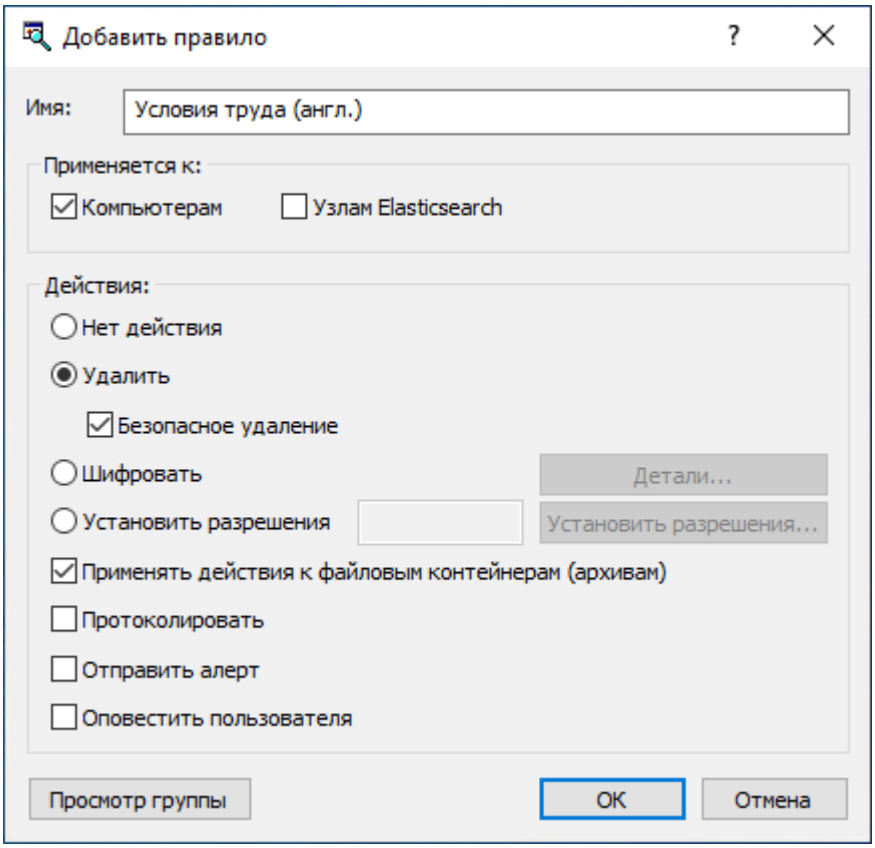
Чтобы удалить правило обнаружения контента

- В нижней части диалогового окна в области **Правила и действия** выберите правило и затем нажмите кнопку **Удалить**, или щелкните правило правой кнопкой мыши и выберите команду **Удалить**.

Узел “Правила и действия”

При обнаружении контента, совпадающего с определенным правилом, Cyber Protego выполняет действие, заданное этим правилом. Используйте диалоговое окно **Редактирование правила**, чтобы просмотреть или изменить действие для этого правила.

1. Откройте консоль Cyber Protego Центральная консоль управления и в дереве консоли выберите **Search and Discovery Server** > **Сервер Discovery** > **Правила и действия**.
2. На панели сведений щелкните по правилу правой кнопкой мыши и выберите **Редактировать** в контекстном меню, чтобы открыть диалоговое окно **Редактирование правила**.



3. Используйте следующие настройки, доступные в диалоговом окне **Редактирование правила**:
   - **Имя** – просмотр или изменение имени правила.
     Имя правила по умолчанию совпадает с именем его контентной группы. При необходимости имя правила может быть изменено.

     Для просмотра контентной группы данного правила нажмите кнопку **Просмотр группы** в левом нижнем углу диалогового окна. Консоль отображает свойства группы в отдельном диалоговом окне, позволяя просматривать свойства, но не изменять их.
   - **Применяется к** – выберите типы подразделений, к которым это правило будет применяться в задачах обнаружения.
     - **Компьютеры** - Правило может использоваться для обнаружения файлов на компьютерах или серверах.
     - **Узлы Elasticsearch** - Правило может использоваться для обнаружения документов в Elasticsearch.

Примечание
Правила, применяемые к узлам Elasticsearch, могут только записывать события в журнал и отправлять алерты. Другие действия в этом случае недоступны.

   - **Не предпринимать действий** – выберите, чтобы оставить обнаруженный контент как есть. Этот вариант следует использовать при настройке правила для протоколирования события обнаружения, алерта или уведомления об обнаружении.
   - **Удалить** – выберите для удаления обнаруженного контента. Доступен следующий вариант:

- **Безопасное удаление** – удаляет обнаруженный контент с использованием безопасной процедуры уничтожения данных по стандарту US DoD 5220.22-M.

- **Шифровать** – выберите для шифрования обнаруженного контента с помощью технологии Windows EFS (Encrypted File System). Чтобы использовать это действие, необходимо настроить шифрование файлов следующим образом.

  a. Выберите параметр **Шифровать**, а затем нажмите кнопку **Сведения**.

  b. В диалоговом окне **Детали шифрования** нажмите **Добавить**.

  c. В открывшемся диалоговом окне выберите сертификат из списка доступных сертификатов шифрования.

  Примечание
  Список доступных сертификатов шифрования соответствует списку личных сертификатов пользователя, под учетной записью которого запущена консоль управления. Личные сертификаты можно просмотреть в оснастке **Сертификаты** консоли управления Microsoft. Дополнительные сведения см. в статье на сайте Microsoft по адресу technet.microsoft.com/library/cc512680.aspx.
  Во время шифрования добавляется сертификат агента восстановления EFS.

  Шифрование не работает при использовании удаленной файловой системы в сканировании без агента или при выполнении сканирования ресурсов SMB. Это ограничение технологии EFS, а не Cyber Protego Discovery.

  Примечание
  Если файл соответствует нескольким правилам с действием **Шифровать**, он будет зашифрован с использованием всех сертификатов, указанных в этих правилах.

- **Установить разрешения** – выберите, чтобы задать разрешения на доступ к файлам для обнаруженного контента. Нажмите кнопку **Установить разрешения**, чтобы открыть стандартное диалоговое окно разрешений файла, предоставляемое операционной системой.

  Примечание
  Если файл соответствует нескольким правилам с действием **Установить разрешения**, итоговые настройки разрешений будут определены путем объединения всех списков управления доступом (ACL) из этих правил.

  Действия при конфликте разрешений: если файл соответствует нескольким правилам со взаимоисключающими разрешениями, итоговый ACL для этого файла будет настроен с индивидуальными параметрами доступа. Допустим, файл соответствует двум правилам, в одном из которых указано Разрешить полный доступ, а в другом указано Запретить запись для одного и того же пользователя. В этом случае итоговый ACL будет следующим: Разрешить: Чтение, Чтение и выполнение; Запретить: Запись.

Если в разных правилах указаны разные пользователи или группы пользователей, то все права управления доступом, заданные этими правилами, объединяются, а итоговый ACL определяется операционной системой Windows.

- **Можно применять действия к файловым контейнерам (архивам)** – выберите, чтобы разрешить применение действия (**Удалить**, **Установить разрешения**, **Шифровать**) ко всему сжатому архиву (например, файлу ZIP или RAR), в котором обнаружен совпадающий контент. Если этот флажок не установлен, действие не будет применяться к контейнеру.

  Примечание
  Этот параметр также распространяется на файлы сохраненных писем (EML), файлы в формате Adobe Portable Document Format (PDF), Rich Text Format (RTF), файлы AutoCAD (.dwg, .dxf) и документы Microsoft Office (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx).

- **Протоколировать** – выберите, чтобы событие обнаружения записывалось в журнал задач (см. Просмотрщик журнала задач).
- **Отправить алерт** – выберите, чтобы оповещать администратора об обнаруженном контенте.
- **Оповестить пользователя** – выберите, чтобы уведомлять пользователя с помощью сообщения в системной области уведомлений.

  Примечание
  Уведомление пользователей недоступно в режиме без агента.

Импорт и экспорт правил

Можно экспортировать все текущие правила и действия обнаружения в файл .dra, который можно затем импортировать на другом компьютере. Можно также импортировать правила и действия обнаружения из файла .dra, а также из контентно-зависимые правила обнаружения из файла контентно-зависимых правил .cwl. Экспорт и импорт могут использоваться также для резервного копирования.

Правила и действия обнаружения можно экспортировать по нажатию кнопки **Сохранить** в диалоговом окне **Правила и действия**. Кнопка **Загрузить** в том же диалоговом окне импортирует правила и действия обнаружения из файла .dra или .swl.

Еще один способ – выбор пункта **Сохранить** и **Загрузить** в узле **Правила и действия** в Cyber Protego Центральная консоль управления.

Экспорт правил и действий обнаружения

1. В дереве консоли раскройте узел **Search and Discovery Server** > **Сервер Discovery** > **Правила и действия**, щелкните правой кнопкой мыши по узлу **Правила и действия**, а затем выберите **Сохранить**.
2. В появившемся диалоговом окне **Сохранить как** укажите файл для экспорта и сохранения экспортируемых правил.
   При экспорте правила сохраняются в файле с расширением .dra.

Импорт правил и действий обнаружения

1. В дереве консоли раскройте узел **Search and Discovery Server** > **Сервер Discovery** > **Правила и действия**, щелкните правой кнопкой мыши по узлу **Правила и действия**, а затем выберите **Загрузить**.
2. В появившемся диалоговом окне **Открыть** укажите файл .dra или .swl, содержащий импортируемые правила.
   За один раз можно импортировать только один файл .dra или .cwl.

Контентно-зависимые правила обнаружения в формате .cwl могут быть загружены из файла. При загрузке правил из файла .cwl параметры **Журнал событий** и **Отправить алерт** автоматически преобразуются в **Журнал** и **Отправить алерт** соответственно. Если исходное правило не имеет этих параметров, то необходимо указать желаемое действие. Такие правила будут показаны с восклицательным знаком.

Внимание
Невозможно использовать список импортированных правил, в котором имеются правила, помеченные восклицательным знаком. Такие правила необходимо настроить заново вручную, назначив им действие или настроив ведение журнала, отправку алертов и уведомлений. После того как все правила правильно настроены, список правил готов к использованию.

Задачи

Cyber Protego Discovery производит все действия (сканирование компьютеров, проверка контента и выполнение действий с обнаруженным контентом) посредством исполнения задач.

Одна лицензия Cyber Protego Discovery позволяет создавать неограниченное число задач. Максимальное число задач ограничено только доступной памятью, процессором и нагрузкой на сеть. Пожалуйста, имейте в виду, что серверу требуется достаточное количество ресурсов для одновременного удаленного подключения по меньшей мере к 10 компьютерам.

Сервер Discovery накладывает следующие ограничения на одновременные соединения:

- Для сканирования посредством агента Discovery:
  - Сервер отправляет задачи удаленным агентам не более чем в 5 потоков единовременно. Данное значение не может быть изменено.
  - Сервер собирает журналы и обновления статуса с удаленных агентов в 10 потоков. Данное значение может быть изменено модификацией следующего значения реестра:
    - Ключ: n Key: HKEY_LOCAL_MACHINE\SOFTWARE\\SmartLine Vision\DeviceLockContentSecurityServer\DiscoverySettings
    - Значение: MaxConcurrentAgents=dword:<количество_потоков>
      Здесь <количество_потоков> должно быть целым числом от 1 до 64.
- Для сканирования в режиме без агента:
  - Сервер сканирует удаленные компьютеры не более чем в 10 потоков единовременно. Данное значение может быть изменено модификацией следующего значения реестра:

- Ключ: HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockContentSecurityServer\DiscoverySettings
- Значение: MaxConcurrentLocalAgents=dword:<количество_потоков>
  Здесь <количество_потоков> должно быть целым числом от 1 до 64.

Во время выполнения задачи происходят следующие действия:

1. Запись информации о статусе в журнал задач (см. Просмотрщик журнала задач), включая данные о подразделениях, сканируемых с помощью Cyber Protego Discovery.
2. Выполнение действий над обнаруженным контентом в соответствии с параметрами, заданными в правилах и действиях Discovery.
3. Создание отчета с информацией об исполнении задачи.

Управление задачами осуществляется посредством Центральной консоли управления, как описано ниже.

Действие	Описание
Просмотр журнала	Чтобы просмотреть журнал задач сервера Discovery: 1. В дереве консоли Cyber Protego раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Задачи**. 2. В узле **Задачи** выберите **Просмотрщик журнала**. Журнал, содержащий информацию о всех задачах, откроется на панели сведений.
Редактирование задачи	Чтобы просмотреть или изменить параметры задачи: 1. В дереве консоли Cyber Protego раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Задачи**. 2. В узле **Задачи** щелкните задачу правой кнопкой мыши и выберите команду **Редактировать задачу** в контекстном меню. Появится мастер, в котором можно просмотреть или изменить параметры задачи.
Просмотр отчета	Чтобы просмотреть отчет для определенной задачи: 1. В дереве консоли Cyber Protego раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Задачи**. 2. В узле **Задачи** раскройте задачу, отчет по которой требуется просмотреть. 3. Выберите нужный отчет в списке под узлом задачи в дереве консоли. Отчет откроется на панели сведений консоли. Каждый отчет привязан к определенной задаче. В связи с этим для просмотра отчетов, созданных различными задачами, потребуется раскрыть каждую задачу и отдельно просмотреть каждый соответствующий отчет.

Узел “Задачи”

Все задачи, а также связанные с ними журнал и отчеты, доступны в дереве консоли в узле **Search and Discovery Server** > **Сервер Discovery** > **Задачи**.

Выбрав узел **Задачи** в дереве консоли, можно увидеть список всех задач сканирования и обнаружения контента. Панель сведений консоли отображает список задач со следующими сведениями по каждой задаче:

- **Имя** - Имя задачи.
- **Статус** - Одно из следующих значений:
  - **Отменена** - Задача была запущена, но остановлена вручную через контекстное меню задачи. Отчеты для отмененных задач не создаются.
  - **Истекла** - Задача была запущена, но от агента не пришел ответ, либо задача была отменена по истечении периода, заданного в параметре Время ожидания агента, для одного или более компьютеров, указанных в задаче.
    Такой статус также назначается задачам, принудительно прерванным по истечении периода, заданного в параметре **Остановить, если выполняется дольше**.
    Во всех таких случаях отчеты задачи создаются на основании информации, полученной от агентов до момента завершения задачи.
  - **Ошибка** - Не удалось выполнить сканирование на всех компьютерах, указанных в задаче (например, все компьютеры были недоступны).
    Отчет задачи в этом случае будет содержать список компьютеров, для которых не удалось выполнить сканирование, с текстом **Не удалось просканировать** и причиной не успешного выполнения сканирования.
  - **Лицензия недоступна** - Задача была запущена, но установленных лицензий оказалось недостаточно для сканирования по крайней мере одного компьютера. По итогам выполнения задачи создается отчет.
  - **Закончена** - Задача была успешно завершена и не требует повторения. По итогам выполнения задачи создается отчет.
  - **Выполняется** - Задача исполняется в данный момент.
  - **Ожидает** - Задача не запускалась и не будет запущена (например, не установлен флаг **Активно**).
  - **По расписанию** - Для задачи задано расписание и она будет запущена в будущем. Данный статус не зависит от того, была ли задача запущена в прошлом.
- **Расписание** - Расписание запуска задачи.
- **Подразделения** - Список подразделений, указанных в задаче.
- **Правила** - Список правил, указанных в задаче.
- **Найдено объектов** - Количество объектов, обнаруженных задачей.
- **Предупреждения** - Количество предупреждений, выданных задачей.
- **Ошибки** - Количество ошибок сканирования, случившихся при исполнении задачи.

Контекстное меню узла **Задачи** содержит следующие команды:

- **Создать задачу** - Создать новую задачу. Параметры задачи можно задать в диалоговых окнах, которые открывает эта команда.

- **Обновить** - Обновить список задач с учетом последних изменений.

Контекстное меню задачи на панели сведений содержит следующие команды:

- **Редактировать задачу** - Просмотреть или изменить параметры задачи. Параметры задачи можно редактировать в диалоговых окнах, которые открывает эта команда.
- **Дублировать задачу** - Создать новую задачу путем копирования параметров выбранной задачи. Параметры новой задачи можно редактировать в диалоговых окнах, которые открывает эта команда.
  Имя новой задачи по умолчанию состоит из префикса **Копия**, за которым следует имя выбранной задачи. При создании двух или более копий к новому имени по умолчанию добавляется числовой суффикс, указывающий номер копии.
- **Удалить задачу** - Удалить выбранную задачу.
  Если данная задача уже запускалась и имеет отчеты, то удалить ее невозможно. Для удаления такой задачи требуется сначала удалить все ее отчеты.
- **Запустить задачу** - Немедленно начать исполнение выбранной задачи. Эта команда применима для любой задачи, кроме уже выполняемых.
- **Остановить задачу** - Немедленно прекратить исполнение выбранной задачи. Эта команда появляется вместо команды **Запустить задачу** для задач, которые в данный момент исполняются.
- **Создать новый отчет** - Инициировать создание отчета. В зависимости от контекста эта команда может быть использована следующим образом:
  - Во время выполнения задачи - Если задача находится в процессе выполнения и есть прогресс, создание отчета невозможно.
  - По завершению задачи - Спустя некоторое время после завершения задачи можно создавать отчеты заново.
    Такая возможность полезна для создания полного отчета по задаче, если она была завершена по истечении периода, определенного параметром Время ожидания агента. В этом случае агенты, которым для завершения своих процессов сканирования потребовалось больше времени, будут передавать данные для журналов на сервер позднее, вне процесса задачи. Сервер в свою очередь будет продолжать собирать эти данные, но отчет не будет пересоздан автоматически. Таким образом, используя команду **Создать новый отчет**, можно получить полные отчеты, содержащую всю доступную информацию о задаче.
- **Обновить** - Обновить список задач с учетом последних изменений.

Создание задачи

Задачи создаются с помощью мастера. Чтобы создать задачу, выполните следующие действия.

1. Откройте мастер создания задачи.
   - В консоли Cyber Protego Центральная консоль управления разверните узел **Search and Discovery Server** > **Сервер Discovery** > **Задачи**, щелкните **Задачи** правой кнопкой мыши и выберите в контекстном меню **Создать задачу**.

2. В открывшемся диалоговом окне **Выбор блоков** выберите блоки, которые будут сканироваться задачей.
   - Выберите один или несколько блоков в списке **Доступные блоки**, а затем нажмите **Добавить**. Чтобы выбрать несколько блоков, удерживайте нажатой клавишу Shift или Ctrl. Добавленные блоки появляются в списке **Выбранные блоки**.

   Для каждого блока в списке отображается его имя и тип. Имя служит для идентификации блока. Тип определяет его назначение: сканирование компьютеров (тип **Компьютеры**) или сканирование узлов Elasticsearch (тип **Узлы Elasticsearch nodes**). Для типа блока **Компьютеры** в квадратных скобках отображается вид списка компьютеров для данного блока: Статический список или Динамический список.

   Для просмотра настроек выбранного блока нажмите кнопку **Просмотр**. В открывшемся диалоговом окне можно увидеть (но не изменить) настройки блока.
3. Нажмите **Далее**, чтобы продолжить.
4. В открывшемся диалоговом окне **Выбор правил и действий** выберите правила, применяемые задачей.
   - Выберите одно или несколько правил в списке **Доступные правила и действия**, а затем нажмите **Добавить**. Чтобы выбрать несколько правил, удерживайте нажатой клавишу Shift или Ctrl. Добавленные правила появляются в списке **Выбранные правила и действия**.

   Для каждого правила список содержит следующую информацию:
   - **Имя правила** – имя, идентифицирующее правило.
   - **Тип правила** – тип контентной группы, используемый данным правилом для обнаружения контента.
   - **Применяется к** – типы блоков, для которых данное правило может быть использовано.
   - **Действия** – идентификаторы действий, которые правило выполняет во время обнаружения контента.

   Список доступных правил ограничен теми правилами, которые применимы к типу блоков, выбранных для данной задачи. Например, если выбраны только блоки Elasticsearch, то список содержит правила, применимые только к узлам Elasticsearch, но не содержит правила для узлов или узлов «Компьютеры» и Elasticsearch и не содержит правила, применимые только к типу «Компьютеры». Если выбраны блоки всех типов, то список содержит все существующие правила.

   Для просмотра настроек выбранного правила нажмите кнопку **Просмотр**. В открывшемся диалоговом окне можно увидеть (но не изменить) настройки правила.
5. Нажмите **Далее**, чтобы продолжить.
6. В диалоговом окне **Настройка расписания задачи и дополнительных параметров** можно изменить имя задачи, настроить задачу для запуска по расписанию, а также задать дополнительные параметры, которые будут влиять на ее выполнение.
   - **Имя задачи** – указывает имя задачи. Под этим именем задача отображается в консоли управления.
   - **Активна** – выберите этот флажок, чтобы активировать задачу согласно расписанию, или сбросьте его, чтобы деактивировать.

Если флажок **Активна** не выбран, то задача не будет выполняться по расписанию.

- **Расписание** – чтобы настроить расписание для задачи, задайте следующие параметры:
  - **Однократно** – задача будет запущена один раз в указанную дату и время. Выберите дату и время запуска задачи либо установите флажок **Сейчас** для запуска задачи сразу после ее создания или изменения.

Примечание
Если указаны дата и время, находящиеся в прошлом, выдается следующее сообщение при нажатии кнопки **Далее**: «Указанная дата раньше текущей даты».

- **Часы** – задача будет выполняться через указанное количество часов. Можно задать количество часов между попытками запуска по расписанию.
- **Дни** – задача будет выполняться через указанное количество дней. Можно задать количество дней между попытками запуска по расписанию.
- **Недели** – задача будет выполняться через указанное количество недель. Можно задать количество недель между попытками запуска по расписанию.
- **Ежемесячно** – задача будет выполняться каждый месяц в указанный день. Можно задать календарные месяцы, в которые задача будет выполняться. Можно также задать числа месяца или дни недели, когда она будет выполняться.

Примечание
При настройке повторяющейся задачи она будет запускаться периодически согласно заданному расписанию. Но если выполнение задачи не завершилось до следующего запуска согласно расписанию, то следующий запуск откладывается до тех пор, пока она не завершится.

- **Дополнительные параметры** – эти параметры позволяют управлять задачей во время выполнения.
  - **Остановить, если выполняется дольше** – указывает, что задача будет принудительно остановлена, если она выполняется дольше указанного периода времени.

Этот параметр позволяет обеспечить успешное выполнение операции, если правила слишком сложны или сканируемые данные слишком объемны и задача не укладывается в расписание.

- **Приоритет сканирования** – указывает приоритет процесса и задает количество одновременно выполняемых потоков в зависимости от числа имеющихся процессоров (ядер).
- При значении **Ниже нормального** или **Низкий** для сканирования будет использоваться только один процессор (ядро), при этом задается приоритет обработки ниже нормального или низкий соответственно.
- При значении **Выше нормального** или **Нормальный** для сканирования будет использоваться половина имеющихся процессоров (ядер), при этом задается приоритет обработки выше нормального или нормальный соответственно.
- При значении **Высокий** будут задействованы все процессоры (ядра), кроме одного, и задан высокий приоритет обработки.

- При значении **Реальное время** задаче сканирования будут выделены все процессоры (ядра) и задан приоритет реального времени для обработки.
- **Количество попыток** – сколько раз будет предпринята попытка, если сканирование возвращает ошибку. Значение 0 означает, что после ошибки больше попытки не предпринимаются.
- **Время ожидания при повторе** – указывает, сколько секунд Cyber Protego будет ждать, прежде чем предпринимать следующую попытку сканирования в случае, если предыдущая попытка завершилась сбоем.
- **Время ожидания агента** – указывает количество часов, в течение которых сервер будет ждать, пока агент не соберет журналы сканирования. Если по истечении этого времени журналы не собраны, то сервер завершает работу этого агента.

Если агент выдает отчет по истечении этого срока или позже, то журналы собираются и обрабатываются как обычно.

7. Нажмите **Далее**. Появляется диалоговое окно подтверждения, содержащее параметры вновь созданной задачи. Нажмите **Готово**, чтобы завершить работу мастера. Вновь созданная задача будет сохранена и запланирована к запуску.

Можно изменять, удалять, дублировать и запускать задачи, обновлять список или формировать новые отчеты через контекстное меню. Описание меню см. в разделе Узел «Задачи» выше в этом документе.

Задача и её отчеты

Задачи сканирования и обнаружения отображаются в дереве консоли под узлом **Search and Discovery Server** > **Сервер Discovery** > **Задачи**.

Контекстное меню задачи в дереве консоли содержит те же команды, что и контекстное меню задачи на панели сведений. Описание команд см. в разделе Узел “Задачи” ранее в этом документе.

Выбрав задачу в дереве консоли, можно увидеть список всех отчетов, созданных этой задачей. Панель сведений консоли отображает список отчетов со следующими сведениями по каждому отчету:

- **Имя** - Имя отчета. По умолчанию содержит имя задачи, а также дату и время ее запуска.
- **Тип** - Возможные значения:
  - **По расписанию** - Отчет создан автоматически по завершении задачи.
  - **Вручную** - Отчет создан пользователем при помощи команды **Создать новый отчет**.
- **Статус** - Возможные значения:
  - **Создание** - Создание отчета продолжается.
  - **Готово** - Отчет создан успешно.
  - **Ошибка** - Отчет завершился с ошибкой.

- **Найдено объектов** - Количество объектов, обнаруженных задачей.
- **Предупреждения** - Количество предупреждений, выданных задачей.
- **Ошибки** - Количество ошибок сканирования, случившихся при исполнении задачи.
- **Запущен** - Дата и время начала создания отчета.
- **Закончен** - Дата и время завершения создания отчета.
- **Запущено** - Учетная запись, запустившая задачу (в случае типа отчета **По расписанию**) или запросившая создание отчета (в случае типа отчета **Вручную**).
- **С компьютера** - Компьютер, с которого была запущена задача (в случае типа отчета **По расписанию**) или запрошено создание отчета (в случае типа отчета **Вручную**).

Контекстное меню отчета на панели сведений содержит следующие команды:

- **Открыть** - Открыть отчет на панели сведений. Эта команда доступна только для уже сформированных отчетов в статусе **Готово** (отмеченных зеленой иконкой).
  Открыть такой отчет можно также выбрав его под узлом задачи в дереве консоли.
- **Показать ошибку** - Вывести информацию об ошибках, произошедших при формировании отчета. Эта команда доступна только для отчетов в статусе **Ошибка** (отмеченных красной иконкой).
- **Переименовать** - Изменить имя отчета. Новое имя можно задать в диалоговом окне, которое открывается этой командой.
- **Удалить отчет** - Удалить выбранный отчет.
  Для удаления нескольких отчетов единовременно выбирайте отчеты щелчком мыши, удерживая нажатой клавишу Shift или Ctrl; затем щелкните правой кнопкой мыши выбранные отчеты и выберите команду **Удалить отчеты**.
- **Создать новый отчет** - Эта команда появляется в меню, если выбрано несколько отчетов. Создает сводный отчет, в котором используется информация из всех выбранных отчетов.
- **Обновить** - Обновляет список отчетов с учетом последних изменений.

Просмотр списка отчетов

При выполнении каждой задачи создается отчет с подробными сведениями о результатах сканирования в понятной пользователю форме. Для доступа к отчетам выполните следующие действия.

1. Откройте консоль управления Cyber Protego Центральная консоль управления.
2. В дереве консоли раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Задачи**.
3. Под узлом **Задачи** выберите и разверните узел, представляющий задачу, отчет которой необходимо открыть.
   Список отчетов данной задачи отображается под узлом этой задачи в дереве консоли, а также на панели сведений справа от него.

Предусмотрены следующие типы отчетов:

- **По расписанию** – отчеты, создаваемые автоматически по завершении задачи.
- **Вручную** – отчеты, создаваемые пользователем вручную с помощью команды **Создать новый отчет**.

Значок в первом столбце указывает статус отчета. Предусмотрены следующие статусы:

- **Создание** – желтый значок. Отчет находится в процессе создания. Подождите завершения процесса, прежде чем открыть отчет.
- **Готово** – зеленый значок. Дважды щелкните по отчету, чтобы открыть его.
- **Ошибка** – красный значок. Дважды щелкните по отчету, чтобы просмотреть сведения об ошибке.

Дополнительные сведения см. в описании списка отчетов в разделе Задача и ее отчеты.

Для управления отчетами выберите один или несколько отчетов на панели сведений, щелкните по выбранным элементам правой кнопкой и выберите нужную команду в контекстном меню. Описание команд приведено в разделе Задача и ее отчеты ранее в этом руководстве.

Примечание
Чтобы выбрать несколько отчетов, удерживайте клавишу Shift или Ctrl.

Просмотр отчета

Раскрыв узел задачи, в дереве консоли можно выбрать любой из отчетов, созданных этой задачей. При выборе отчета в дереве консоли, панель сведений отображает страницы отчета. Отобразить отчет можно также командой **Открыть** из контекстного меню или двойным щелчком в списке отчетов на панели сведений консоли.

Контекстное меню отчета в дереве консоли содержит следующие команды:

- **Открыть** - Отобразить отчет на панели сведений.
- **Переименовать** - Изменить имя отчета. Новое имя можно задать в диалоговом окне, которое открывается этой командой.
- **Удалить отчет** - Удалить выбранный отчет.
- **Обновить** - Обновить отчет на панели сведений консоли.

Сервер Discovery создает отчеты в многостраничном виде в формате HTML.

Примечание
Если JavaScript не включен в вашем веб-браузере, при просмотре отчетов появится следующее сообщение об ошибке: “Для полной функциональности этой страницы необходимо включить JavaScript. Смотрите руководство вашего веб-браузера или справку о том, как включить JavaScript.”

Для просмотра отчетов необходимо включить JavaScript. Инструкции см. в руководстве “Как включить JavaScript в вашем веб-браузере” по адресу www.enable-javascript.com/ru/.

Сервер Discovery позволяет создавать отчеты по результатам сканирования в автоматическом режиме или вручную. Отчеты представляют в удобной форме информацию об обнаруженном контенте и действиях, выполненных в ходе сканирования.

Обычно отчеты создаются задачами автоматически. Кроме того, их можно создавать вручную в Центральной консоли управления.

Каждый отчет содержит детальную информацию о результатах сканирования.

Первая страница отчета может содержать следующую информацию:

- **Заголовок отчета** - В заголовке отображается имя отчета, а также содержится информация о начале и завершении сканирования, имени пользователя, запросившего отчет, и имени компьютера, с которого было инициировано создание отчета.
- **Результаты Discovery** - Результаты обнаружения, включающие сводную информацию о результатах сканирования и действиях, выполненных над обнаруженным контентом. Если задачей не были обнаружены определенные данные, этот раздел отчета содержит текст **Результаты Discovery: Нет**.
  Сводная информация в данном разделе отчета включает:
  - **Имя объекта** - Перечисление правил и подразделений, в которых был обнаружен контент, отвечающий перечисленным правилам.

  В списке подразделений и правил отображаются следующие сведения:

- **Протоколирование** - Общее количество событий обнаружения, отраженных в журнале.
- **Алерт** - Общее количество тревожных алертов об обнаружении контента, отправленных администратору.
- **Алерт** - Общее количество показанных уведомлений об обнаружении контента.
- **Удаление** - Общее количество действий удаления обнаруженного контента.
- **Шифрование** - Общее количество действий шифрования файлов, содержащих обнаруженный контент.
- **Задание разрешений** - Общее количество действий изменения разрешений на файлы, содержащие обнаруженный контент.
- **Предупреждения** - Общее количество событий с ошибками, таких как ошибка доступа к файлу, ошибка контентного анализа, ошибка применения действий к обнаруженным файлам.
- **Правила** - В этом разделе содержится описание всех правил, включенных в задачу, в том числе не показанных в разделе **Результаты Discovery**.
- **Не удалось просканировать** - Если задаче обнаружения не удалось просканировать какие-либо из ее целевых ресурсов (компьютеров и/или узлов Elasticsearch), в отчете содержится сводная информация об ошибках:
  - **Подразделение/Ресурс** - Перечень подразделений с компьютерами или узлами, которые не удалось просканировать.
  - **Ошибка** - Описание ошибки, из-за которой компьютер или узел не удалось просканировать.
  - **Дата/Время** - Дата и время возникновения ошибки.

Примечание

Многие пункты отчета являются активными элементами. Щелчок мыши на таком элементе открывает страницу с информацией по выбранному элементу отчета, либо открывает просмотрщик журнала задач с фильтром, настроенным на отображение всех связанных с выбранным пунктом отчета записей журнала. Например, если щелкнуть число в строке **Всего**, откроется просмотрщик журнала задач со сведениями о всех подсчитанных в сводной таблице отчета действиях.

Подробнее о работе с отчетами см. в разделе Навигация по отчетам.

Раскрыть любой объект отчета можно, щелкнув значок **[+]** слева от объекта. Чтобы раскрыть все объекты, щелкните значок **[+]** слева от заголовка **Имя объекта**.

Дальнейшие страницы отчета содержат детализированную информацию, включая следующие разделы:

- **Заголовок отчета** - В заголовке отображается имя отчета, а также содержится информация о начале и завершении сканирования, имени пользователя, запросившего отчет, и имени компьютера, с которого было инициировано создание отчета.
- **Результаты Discovery** - В этом разделе перечисляются просканированные ресурсы (компьютеры и узлы Elasticsearch). Список можно раскрыть, щелкнув имя ресурса. В результате появится список обнаруженных файлов.

  Примечание

  Предусмотрено два варианта отображения списка ресурсов и файлов. В первом варианте выводятся имена ресурсов, к которым относятся файлы. Во втором - сначала отображаются имена файлов, развернув которые, можно увидеть ресурсы, на которых эти файлы были обнаружены. Вид списка зависит от типа ссылки, выбранной для получения данного отчета. Подробнее об отображения элементов отчета см. в разделе Навигация по отчетам.

  Сводная информация в данном разделе отчета включает:

  - **Имя объекта** - Отображаются имена ресурсов и имена файлов, в зависимости от режима просмотра. Перечисляются либо ресурсы, с каждым из которых связан список обнаруженных на нем файлов, либо файлы, с каждым из которых связан список ресурсов, на которых этот файл был обнаружен.

  В списке ресурсов и файлов отображаются следующие сведения:

- **Протоколирование** - Общее количество событий обнаружения, отраженных в журнале.
- **Алерт** - Общее количество тревожных алертов об обнаружении контента, отправленных администратору.
- **Алерт** - Общее количество показанных уведомлений об обнаружении контента.
- **Удаление** - Общее количество действий удаления обнаруженного контента.
- **Шифрование** - Общее количество действий шифрования файлов, содержащих обнаруженный контент.

- **Задание разрешений** - Общее количество действий изменения разрешений на файлы, содержащие обнаруженный контент.
- **Предупреждения** - Общее количество событий с ошибками, таких как ошибка доступа к файлу, ошибка контентного анализа, ошибка применения действий к обнаруженным файлам.

Примечание

Некоторые пункты отчета являются активными элементами. Так, щелчок мыши на имени файла или ресурса раскрывает связанный с ним список ресурсов или файлов, а по щелчку на подчеркнутых числовых значениях открывается просмотрщик журнала задач.

Подробнее о работе с отчетами см. в разделе Навигация по отчетам.

Предусмотрен также вариант простого табличного отчета, в котором перечисляются либо все обнаруженные файлы, либо все ресурсы, где был обнаружен хотя бы один файл с искомым контентом. В таком отчете отсутствуют вложенные списки разных уровней, но щелчком на файле можно открыть список ресурсов, на которых данный файл был обнаружен, а щелчком на ресурсе можно открыть список файлов, обнаруженных на данном ресурсе.

В простом табличном отчете предоставляется следующая информация:

- **Заголовок отчета** - В заголовке отображается имя отчета, а также содержится информация о начале и завершении сканирования, имени пользователя, запросившего отчет, и имени компьютера, с которого было инициировано создание отчета.
- **Результаты Discovery** - Список файлов и ресурсов (компьютеров и узлов Elasticsearch), обнаруженных в соответствии с заданными правилами и подразделениями. Список может быть представлен в одном из следующих видов, в зависимости от способа перехода к отчету:
  - **Имя объекта**:
    - **Ресурсы для** <имя файла> **для** <имя подразделения> **и** <имя правила> - Перечисляются ресурсы, на которых был обнаружен указанный файл в указанном подразделении в соответствии с указанным правилом.

      - или -
    - **Ресурсы для** <имя файла> **для** <имя правила> - Перечисляются ресурсы, на которых был обнаружен указанный файл в соответствии с указанным правилом.

      - или -
    - **Данные для** <имя ресурса> **для** <имя подразделения> **и** <имя правила> - Перечисляются файлы, обнаруженные на указанном ресурсе в указанном подразделении в соответствии с указанным правилом.

      - или -
    - **Данные для** <имя ресурса> **для** <имя правила> - Перечисляются файлы, обнаруженные на указанном ресурсе в соответствии с указанным правилом. Если какой-либо файл имеет более одного имени (различные псевдонимы или альтернативные имена), в скобках после имени файла будет указано количество псевдонимов.

Во всех перечисленных вариантах представления списка имена файлов, ресурсов, правил и подразделений указываются переменными <имя файла>, <имя ресурса>, <имя правила> и <имя подразделения> соответственно.

В списке ресурсов и файлов отображаются следующие сведения:

- **Протоколирование** - Общее количество событий обнаружения, отраженных в журнале.
- **Алерт** - Общее количество тревожных алертов об обнаружении контента, отправленных администратору.
- **Алерт** - Общее количество показанных уведомлений об обнаружении контента.
- **Удаление** - Общее количество действий удаления обнаруженного контента.
- **Шифрование** - Общее количество действий шифрования файлов, содержащих обнаруженный контент.
- **Задание разрешений** - Общее количество действий изменения разрешений на файлы, содержащие обнаруженный контент.
- **Предупреждения** - Общее количество событий с ошибками, таких как ошибка доступа к файлу, ошибка контентного анализа, ошибка применения действий к обнаруженным файлам.

Еще один тип отчета - просмотр по псевдонимам файла. Если обнаружено несколько файлов с одинаковым содержимым, но под разными именами, эти имена называются псевдонимами. В данном отчете перечисляются все псевдонимы обнаруженных файлов. Щелкнув псевдоним файла или значок **[+]** слева от него, можно раскрыть список ресурсов (компьютеров и узлов Elasticsearch), на которых данный файл был обнаружен.

Отчет по псевдонимам содержит две таблицы. Первая - таблица псевдонимов, вторая - список ресурсов (компьютеров и узлов Elasticsearch), на которых был обнаружен файл с псевдонимом из первой таблицы. В отчете по псевдонимам предоставляется следующая информация:

- **Заголовок отчета** - В заголовке отображается имя отчета, а также содержится информация о начале и завершении сканирования, имени пользователя, запросившего отчет, и имени компьютера, с которого было инициировано создание отчета. Заголовок содержит также информацию о подразделении, правиле и ресурсе, для которого был создан данный отчет.
- **Псевдонимы** - Список всех псевдонимов (различных имен одного и того же файла), обнаруженных на указанном ресурсе в соответствии с заданными правилами и подразделениями. В этом списке перечисляются:
  - **Имя объекта** - Все имена обнаруженного файла. Для каждого имени приводится список ресурсы, на которых данный файл был обнаружен под этим именем.

  В списке файлов отображаются следующие сведения:

- **Протоколирование** - Общее количество событий обнаружения, отраженных в журнале.
- **Алерт** - Общее количество тревожных алертов об обнаружении контента, отправленных администратору.
- **Алерт** - Общее количество показанных уведомлений об обнаружении контента.
- **Удаление** - Общее количество действий удаления обнаруженного контента.

- **Шифрование** - Общее количество действий шифрования файлов, содержащих обнаруженный контент.
- **Задание разрешений** - Общее количество действий изменения разрешений на файлы, содержащие обнаруженный контент.
- **Предупреждения** - Общее количество событий с ошибками, таких как ошибка доступа к файлу, ошибка контентного анализа, ошибка применения действий к обнаруженным файлам.

- **Результаты Discovery** - Список ресурсов, на которых обнаружен данный файл под именами, указанными в таблице псевдонимов. В этом списке:
  - **Имя объекта** - Все ресурсы, содержащие определенный файл, перечислены под соответствующим именем файла.

  В списке ресурсов и файлов отображаются следующие сведения:

- **Протоколирование** - Общее количество событий обнаружения, отраженных в журнале.
- **Алерт** - Общее количество тревожных алертов об обнаружении контента, отправленных администратору.
- **Алерт** - Общее количество показанных уведомлений об обнаружении контента.
- **Удаление** - Общее количество действий удаления обнаруженного контента.
- **Шифрование** - Общее количество действий шифрования файлов, содержащих обнаруженный контент.
- **Задание разрешений** - Общее количество действий изменения разрешений на файлы, содержащие обнаруженный контент.
- **Предупреждения** - Общее количество событий с ошибками, таких как ошибка доступа к файлу, ошибка контентного анализа, ошибка применения действий к обнаруженным файлам.

Навигация по отчетам

Отчеты Discovery обладают развитой структурой навигации. По большинству пунктов отчета можно получить дальнейшую детализацию, выбирая пункт отчета щелчком мыши. Кроме того, многие элементы отчета являются активными. По щелчку на активном элементе открывается другая страница отчета (детализированный просмотр информации для выбранного элемента) или журнал задач с предустановленным фильтром для отображения записей, относящихся к выбранному элементу.

Раздел отчета “Результаты Discovery”

Первый столбец таблицы **Результаты Discovery** содержит пункты, являющиеся активными элементами. По щелчку на правиле или подразделении появляется контекстное меню.

Если щелкнуть мышью на правиле, в контекстном меню будут доступны следующие команды:

- **Ресурсы для правила** - Отобразить список всех ресурсов (компьютеры и узлы Elasticsearch), на которых был обнаружен контент, отвечающий данному правилу.
- **Данные для правила** - Отобразить список всех файлов, в которых был обнаружен контент, отвечающий данному правилу.

Если раскрыть правило и выбрать одно из подразделений, в контекстом меню будут доступны следующие команды:

- **Ресурсы для подразделения и правила** - Отобразить список ресурсов из выбранного подразделения, на которых был обнаружен контент, отвечающий данному правилу.
- **Данные для подразделения и правила** - Отобразить список файлов, расположенных на ресурсах из данного подразделения, в которых был обнаружен контент, отвечающий данному правилу.

Некоторые числа в таблице отчета являются активными элементами. При наведении указателя мыши на такое число под ним появляется подчеркивание, а щелчок мыши на таком числе открывает просмотрщик журнала задач, как описано в разделе **Переход к журналу задач**.

Раздел отчета “Не удалось просканировать”

В разделе **Не удалось просканировать** перечисляются все подразделения с ресурсами (компьютеры и узлы Elasticsearch), на которых не удалось выполнить сканирование. Щелчок мыши на подразделении открывает список таких проблемных ресурсов с соответствующими сообщениями об ошибках. Возможны следующие сообщения об ошибках:

- **Компьютер недоступен** - Во время сканирования целевой компьютер или сервер был недоступен (например, выключен или не подключен к сети).
- **Ошибка установки** - Не удалось установить агент Discovery на целевой компьютер.
- **Доступ запрещен** - При попытке доступа к сканируемому ресурсу возникла проблема с с настроенными учетными данными для доступа или сертификатом.
- **Лицензия недоступна** - Количество сканируемых ресурсов превысило лицензию. Для сканирования большего количества ресурсов требуется дополнительная лицензия.

Детализированная таблица

При выборе одного из четырех пунктов меню, описанных выше (см. Раздел отчета “Результаты Discovery”), открывается соответствующая детализированная таблица отчета. Щелчок по имени ресурса раскрывает список файлов, обнаруженных соответствующим правилом на этом ресурсе. Щелчок по имени файла отображает список ресурсов, на которых этот файл был обнаружен соответствующим правилом. Выбранный вариант отображения списка указывается в строке **Результаты Discovery**.

Некоторые числа в детализированной таблице являются активными элементами. При наведении указателя мыши на такое число под ним появляется подчеркивание, а щелчок мыши на таком числе открывает просмотрщик журнала задач, как описано в разделе **Переход к журналу задач**.

Количество отображаемых в таблицах записей регулируется следующими значениями реестра:

- Ключ: HKEY_CURRENT_USER\SOFTWARE\SmartLine Vision\DLManager\Manager
  - Значение: DisplayRootCount=dword:<количество корневых элементов>
    Значение по умолчанию равно 500.

- Значение: DisplayChildCount=dword:<количество дочерних элементов>
  Значение по умолчанию равно 50.

По умолчанию в отчет выводится до 500 элементов верхнего уровня (корневых элементов) и до 50 дочерних для каждого из корневых элементов.

Раздел отчета “Правила”

Раздел отчета **Правила** содержит список правил, использованных при сканировании. По щелчку на имени правила происходит переход в узел дерева консоли **Правила и действия** с автоматическим выбором этого правила на панели сведений консоли.

Переход к журналу задач

Дополнительную информацию о каком-либо пункте в таблицах отчета можно получить, щелкнув мышью на подчеркнутом пункте в заголовке или на подчеркнутом числе в таблице. В результате откроется просмотрщик журнала задач, при этом фильтр журнала будет настроен на отображение записей, относящихся к выбранному элементу отчета.

Правило фильтрации использует логический оператор И для объединения всех полей, относящихся к выбранному элементу отчета, и выглядит следующим образом:

<ID отчета> И <имя поля> И <имя правила> И <имя подразделения>

Полученный фильтр применяется к журналу, так что отображаются только записи, удовлетворяющие правилу фильтрации. В результате просмотрщик журнала задач всегда отображает информацию, релевантную выбранному элементу в отчете. При необходимости можно использовать команду **Сбросить фильтр** для сброса фильтра и просмотра журнала в полном объеме.

Просмотрщик журнала задач

Этот просмотрщик позволяет просматривать файлы журнала, созданные задачами обнаружения. Задачи обнаружения используют этот журнал для записи сведений о действиях сканирования, обнаружении контента и действиях, примененных к обнаруженному контенту.

Для доступа к журналу задач выполните следующие действия.

1. Откройте консоль управления Cyber Protego Центральная консоль управления.
2. В дереве консоли разверните узел **Search and Discovery Server** > **Сервер Discovery** > **Задачи**, а затем выберите **Просмотрщик журнала** под узлом **Задачи**.

На панели сведений отобразится список событий со следующей информацией о каждом из событий:

- **Тип** - Тип события. Возможные значения:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.

- **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
- **Ошибка** - Произошла ошибка.

- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Имя задачи** – указывает задачу обнаружения, вызвавшую событие.
- **Расположение** – имя ресурса, с которым связано событие.
- **Действия** – указывает действие с обнаруженным контентом, выполняемое задачей, например:
  - **Алерт** – отправка тревожного алерта об обнаруженном контенте.
  - **Удалить** – удаление обнаруженного контента.
  - **Удалить (безопасное удаление)** – удаление с использованием безопасной процедуры уничтожения данных по стандарту US DoD 5220.22-M.
  - **Шифровать** - Шифрование обнаруженного контента с помощью технологии Windows EFS (Encrypted File System).
  - **Протоколировать** – запись информации об обнаруженном контенте в журнал задач сервера Discovery.
  - **Оповестить** – алерт пользователя компьютера об обнаруженном контенте.
  - **Установить разрешения** – настройка определенных разрешений файловой системы для обнаруженных файлов.
- **Имя** – имя обнаруженного файла.
- **Причина** – причина возникновения события, например:
  - **Завершено** – завершение задачи обнаружения.
  - **Ошибка контентно-зависимого правила** – ошибка применения правила обнаружения.
  - **По запросу** – задача обнаружения запущена вручную.
  - **По расписанию** – задача обнаружения запущена по расписанию.
  - **Правило** – сработавшее правило обнаружения. В причине указано имя правила и краткое описание совпадений контента, ключевых слов и/или типов файлов, которые привели к срабатыванию правила.
- **Информация** – описание события с подробными сведениями о выполненных действиях и возникших ошибках.
- **Подразделение** – название подразделения, в котором возникла ошибка.
- **Тип подразделения** – целевое назначение подразделения, в котором произошло событие: сканирование компьютеров (тип **Компьютеры**) или сканирование узлов Elasticsearch (тип **Узлы Elasticsearch**).
- **Дата/Время сбора** – дата и время получения события сервером Cyber Protego Discovery.

Управление журналом задач

Для управления журналом служат команды контекстного меню:

- В дереве консоли раскройте узлы **Search and Discovery Server** > **Сервер Discovery** > **Задачи**, а затем щелкните правой кнопкой мыши по пункту **Просмотрщик журнала** под узлом **Задачи**.
  - или -
  В дереве консоли выберите **Search and Discovery Server** > **Сервер Discovery** > **Задачи** > **Просмотрщик журнала** и щелкните правой кнопкой мыши по какую-либо записи в списке на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

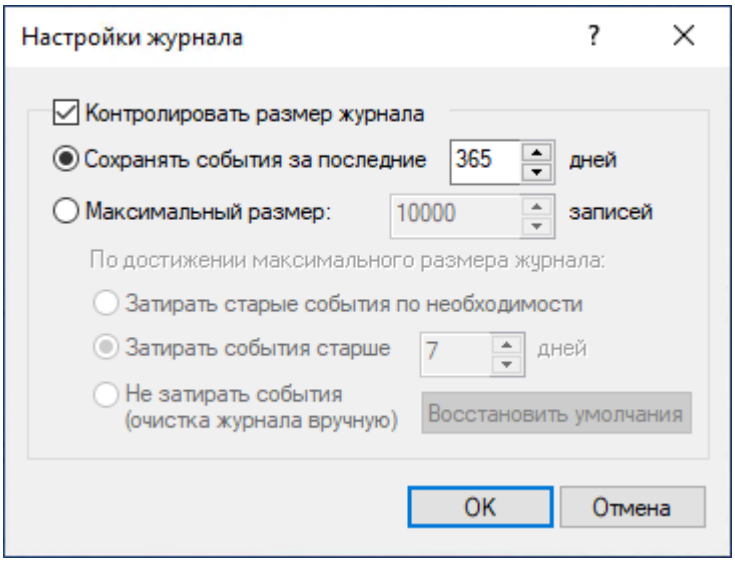
- **Настройки** – просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. инструкцию Чтобы просмотреть или изменить настройки журнала задач Discovery).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Копировать строку** - Копировать содержимое выделенной строки журнала в буфер обмена.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** – отображать только записи о событиях, которые удовлетворяют заданным условиям (см. инструкцию Чтобы настроить фильтр журнала задач Discovery).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.
  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Чтобы просмотреть или изменить настройки журнала задач Discovery

1. Выберите команду **Настройки** в контекстном меню.
2. Просмотрите или измените настройки журнала в появившемся диалоговом окне.



Предусмотрены следующие настройки журнала:

- **Контролировать размер журнала** - Установите этот флажок, чтобы разрешить серверу контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, сервер использует все доступное пространство базы данных для хранения журнала.
- **Сохранять события за последние** <число> **дней** - Выберите этот параметр, чтобы хранить записи не старше определенного количества дней. Затем задайте нужное количество дней. Значение по умолчанию - 365 дней.
- **Максимальный размер:** <число> **записей** – сохранять не более определенного количества записей. При выборе этого параметра укажите нужное количество записей и выберите действие сервера, которое будет выполняться, когда журнал достигнет максимального размера.
  - **Затирать старые события по необходимости** - Новые записи событий продолжают сохраняться при достижении максимального размера журнала. Каждая запись нового события заменяет собой самую старую запись в журнале.
  - **Затирать события старше** <число> **дней** - Новые записи событий заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
  - **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи событий не добавляются. Чтобы обеспечить их добавление, необходимо очистить журнал вручную.

Внимание

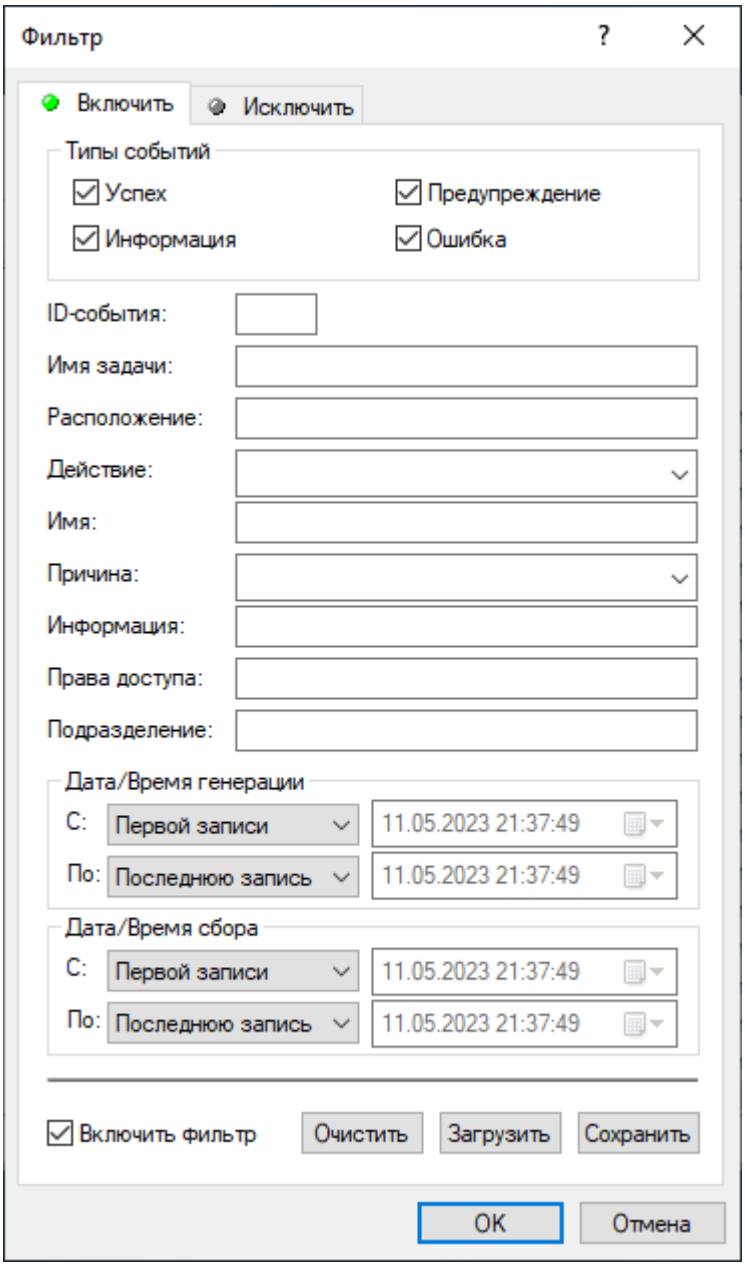
Если в журнале нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер не будет добавлять новые записи в журнал.

Чтобы использовать настройки по умолчанию, выберите параметр **Максимальный размер** и нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:

- Максимальный размер: 10 000 записей
- Затирать события старше 7 дней

Чтобы настроить фильтр журнала задач Discovery

1. Выберите команду **Фильтр** в контекстном меню.
2. Просмотрите или измените параметры фильтра в появившемся диалоговом окне.



Предусмотрены фильтры двух типов:

- **Включить** - Отображать в списке только события, удовлетворяющие условиям, заданным на вкладке **Включить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке Включить.
- **Исключить** - Не отображать в списке события, удовлетворяющие условиям, заданным на вкладке **Исключить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке Исключить.

Фильтр можно временно выключить. Для этого снимите флажок **Включить фильтр**.

Примечание
Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно его настроить, задав необходимые значения в следующих полях:

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- Строковые поля, которые позволяют включать или исключать события в зависимости от того, соответствуют ли данные события указанной строке фильтра. Например, для фильтрации событий по имени задачи, вызвавшей событие, задайте строку фильтра в поле **Имя задачи**. Для фильтрации событий с определенными ID-номерами введите номера искомых событий в поле **ID-события**, разделяя их точкой с запятой.
  Предусмотрены следующие строковые поля:
  - **ID-события** – идентификационный номер события.
  - **Имя задачи** – имя задачи, вызвавшей событие.
  - **Расположение** – имя ресурса, с которым связано событие.
  - **Действие** – имя действия, которое вызвало событие. Здесь можно ввести имя или выбрать его из следующего списка:
    - **Алерт** – отправка алерта об обнаруженном контенте.
    - **Удаление** – удаление обнаруженного контента.
    - **Удаление (безопасное удаление)** – удаление с помощью процедуры безопасного стирания, определенной в стандарте Министерства обороны США 5220.22-M.
    - **Шифрование** – шифрование обнаруженного контента с помощью Windows EFS (Encrypted File System).
    - **Протоколирование** – запись в журнал задач Discovery события, которое уведомляет об обнаруженном контенте.

    - **Алерт** – алерт пользователя компьютера об обнаруженном контенте.
    - **Установка разрешений** – задание определенных разрешений файловой системы для обнаруженных файлов.
  - **Имя** – имя обнаруженного файла.
  - **Причина** – причина, которая привела к инициации события. Причину можно ввести или выбрать ее из следующего списка:
    - **Завершено** – завершение задачи обнаружения.
    - **Ошибка контентно-зависимого правила** – ошибка применения правила обнаружения.
    - **По запросу** – задача обнаружения запущена вручную.
    - **По расписанию** – задача обнаружения запущена по расписанию.
    - **Правило** – применение правила обнаружения.
  - **Информация** – подробное описание события, включая описание выполненных действий и возникших ошибок.
  - **Подразделение** – название подразделения, в котором возникла ошибка.

Примечание
Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

- **Дата/время создания** – в этой области можно с помощью следующих полей указать требуемый диапазон дат и времени возникновения события:
  - **С** – начало временного интервала событий для фильтрации. Возможные значения: **Первой записи** (значение по умолчанию) и **Записи от**. Выберите **Первой записи**, чтобы фильтровать события, начиная с самого первого созданного события. Выберите **Записи от**, чтобы фильтровать события, произошедшие не ранее определенных даты и времени.
  - **По** – конец временного интервала событий для фильтрации. Возможные значения: **Последнюю запись** (значение по умолчанию) и **Записи от**. Выберите **Последнюю запись**, чтобы фильтровать события, заканчивая последним созданным событием. Выберите **Записи от**, чтобы фильтровать события, произошедшие не позднее определенных даты и времени.
- **Дата/время получения** – в этой области можно с помощью следующих полей указать требуемый диапазон дат и времени, в которые событие было принято сервером Discovery Server:
  - **С** – начало временного интервала событий для фильтрации. Возможные значения: **Первой записи** (значение по умолчанию) и **Записи от**. Выберите **Первой записи**, чтобы фильтровать события, начиная с самого первого принятого события. Выберите **Записи от**, чтобы фильтровать события, принятые не ранее определенных даты и времени.
  - **По** – конец временного интервала событий для фильтрации. Возможные значения: **Последнюю запись** (значение по умолчанию) и **Записи от**. Выберите **Последнюю запись**,

чтобы фильтровать события, заканчивая последним принятым событием. Выберите **Записи от**, чтобы фильтровать события, принятые не позднее определенных даты и времени.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Просмотрщик журнала Discovery

Этот просмотрщик позволяет получить доступ к внутреннему журналу сервера Cyber Protego Discovery. Сервер использует этот журнал для регистрации ошибок, предупреждений и другой важной информации (такой как данные об изменениях конфигурации, событиях запуска/останова и т. п.). В отличие от журнала задач, журнал Discovery содержит информацию, которая не относится напрямую к задачам сканирования.

Информация из этого журнала может быть полезной для диагностики и выявления проблем в работе сервера, а также для контроля изменений в его настройках и действий по очистке журналов.

Чтобы открыть журнал сервера Cyber Protego Discovery, выполните следующие действия.

1. Откройте консоль управления Cyber Protego Центральная консоль управления.
2. В дереве консоли Cyber Protego Центральная консоль управления раскройте узлы **Search and Discovery Server** > **Сервер Discovery**, затем выберите элемент **Просмотрщик журнала Discovery** под узлом **Сервер Discovery**.

На панели сведений отобразится список событий со следующей информацией о каждом из событий:

- **Тип** - Тип события. Возможные значения:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.

- **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
- **Ошибка** - Произошла ошибка.

- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Информация** – подробное описание события, включая описание выполненных действий и возникших ошибок.
- **Сервер** - Имя компьютера, на котором произошло событие.
- **Запись N** - Порядковый номер события в списке.

Управление журналом Discovery

Для управления журналом служат команды контекстного меню:

- В дереве Центральной консоли управления раскройте узлы **Search and Discovery Server** > **Сервер Discovery**, и щелкните правой кнопкой мыши элемент **Просмотрщик журнала Discovery** под узлом **Сервер Discovery**.

  - или -

- В дереве Центральной консоли управления выберите **Search and Discovery Server** > **Сервер Discovery** > **Просмотрщик журнала Discovery** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. инструкцию Чтобы просмотреть или изменить настройки журнала Discovery).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Копировать строку** - Копировать содержимое выделенной строки журнала в буфер обмена.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. инструкцию Чтобы настроить фильтр журнала Discovery).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

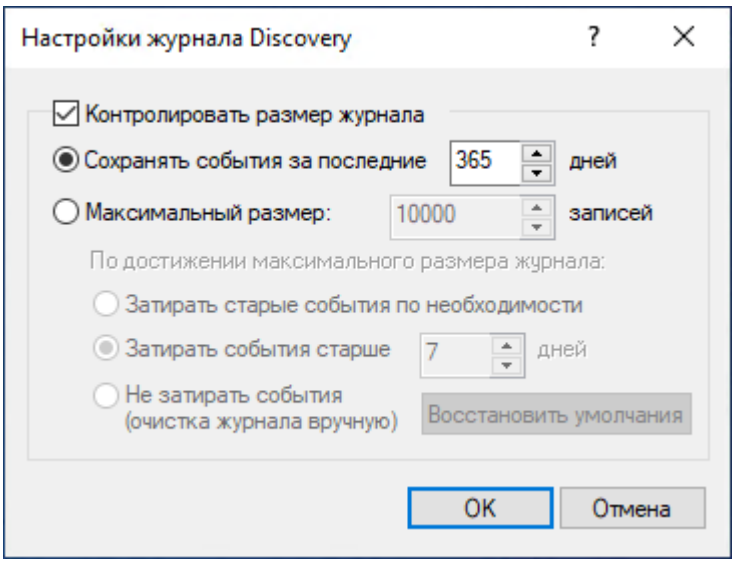
Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).

- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.
  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Чтобы просмотреть или изменить настройки журнала Discovery

1. Выберите команду **Настройки** в контекстном меню.
2. Просмотрите или измените настройки журнала в появившемся диалоговом окне.



Предусмотрены следующие настройки журнала:

- **Контролировать размер журнала** - Установите этот флажок, чтобы разрешить серверу контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, сервер использует все доступное пространство базы данных для хранения журнала.
- **Сохранять события за последние** <число> **дней** - Выберите этот параметр, чтобы хранить записи не старше определенного количества дней. Затем задайте нужное количество дней. Значение по умолчанию - 365 дней.
- **Максимальный размер:** <число> **записей** - Выберите этот параметр, чтобы хранить не более определенного количества записей. Затем укажите нужное количество записей и выберите действие сервера, которое будет выполняться, когда журнал достигнет максимального размера:

- **Затирать старые события по необходимости** - Новые записи событий продолжают сохраняться при достижении максимального размера журнала. Каждая запись нового события заменяет собой самую старую запись в журнале.
- **Затирать события старше** <число> **дней** - Новые записи событий заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
- **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи событий не добавляются. Чтобы обеспечить их добавление, необходимо очистить журнал вручную.

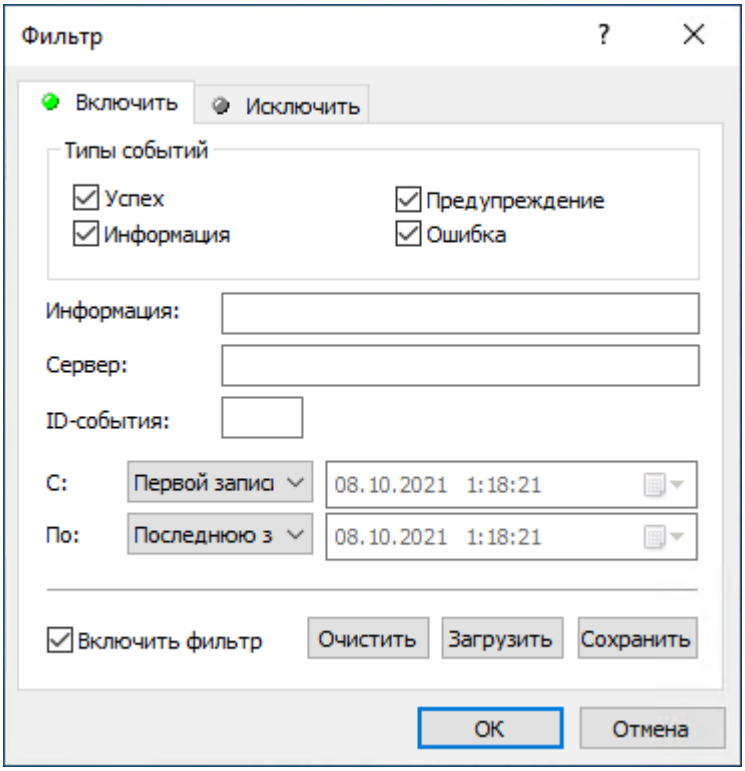
Внимание
Если в журнале нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер не будет добавлять новые записи в журнал.

Чтобы использовать размер журнала по умолчанию, выберите параметр **Максимальный размер** и нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:

- Максимальный размер: 10 000 записей
- Затирать события старше 7 дней

Чтобы настроить фильтр журнала Discovery

1. Выберите команду **Фильтр** в контекстном меню.
2. Просмотрите или измените параметры фильтра в появившемся диалоговом окне.



Предусмотрены фильтры двух типов:

- **Включить** - Отображать в списке только события, удовлетворяющие условиям, заданным на вкладке **Включить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке Включить.
- **Исключить** - Не отображать в списке события, удовлетворяющие условиям, заданным на вкладке **Исключить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке Исключить.

Для временного отключения фильтра снимите флажок **Включить фильтр**.

Примечание
Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно его настроить, задав необходимые значения в следующих полях:

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- **Информация**, **Сервер**, **ID-события** - Включение или исключение из списка событий, у которых в указанном поле данных встречается заданная строка. Например, для фильтрации событий по имени компьютера, на котором произошло событие, укажите строку фильтра в поле **Сервер**. Для фильтрации событий с определенными номерами, введите номера искомых событий в поле **ID-события**, используя точку с запятой в качестве разделителя.

  Примечание
  Чтобы облегчить настройку фильтра, строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

- **С** - Начало временного интервала событий для фильтрации. Возможные значения: **Первой записи** (значение по умолчанию) и **Записи от**. Выберите **Первой записи**, чтобы фильтровать события, начиная с самого раннего в журнале. Выберите **Записи от**, чтобы фильтровать события, произошедшие не ранее определенной даты и времени.
- **По** - Конец временного интервала событий для фильтрации. Возможные значения: **Последнюю запись** (значение по умолчанию) и **Записи от**. Выберите **Последнюю запись**, чтобы фильтровать события, заканчивая самым поздним в журнале. Выберите **Записи от**, чтобы фильтровать события, произошедшие не позднее определенной даты и времени.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Указатель