Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра защиты информации

СИСТЕМА ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ДАННЫХ «КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM»

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1-98 80 01 «Информационная безопасность»

Минск БГУИР 2021

Библиотека БГУИР

УДК 004.056.5(076)
ББК 32.972.5я73
С40

А в т о р ы:

Т. В. Борботько, О. В. Бойправ, В. Е. Морозов, А. В. Дрозд

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем
учреждения образования «Белорусская государственная академия связи»
(протокол №9 от 05.03.2020);

начальник научно-исследовательской лаборатории
кафедры автоматизированных систем управления войсками
учреждения образования «Военная академия Республики Беларусь»
кандидат технических наук, доцент А. В. Хижняк

Система противодействия утечке данных «Контур информационной
С40 безопасности SearchInform» : пособие / Т. В. Борботько [и др.]. – Минск :
БГУИР, 2021. – 284 с. : ил.
ISBN 978-985-543-587-8.

Обосновывается важность использования современных средств защиты от внутренних угроз информационной безопасности, раскрываются преимущества DLP-систем перед альтернативными решениями, рассматриваются принципы построения и технологии, лежащие в основе функционирования DLP-систем. Подробно описываются архитектура, особенности применения и аналитические возможности DLP-системы «Контур информационной безопасности SearchInform». Даны рекомендации по формированию типовых политик безопасности применительно к различным ситуациям, возникающим в деятельности современных организаций и предприятий.

Предназначено для студентов образовательных учреждений высшего профессионального образования, изучающих дисциплину «Система противодействия утечке данных», руководителей и сотрудников служб информационной безопасности, а также широкого круга читателей, интересующихся вопросами обеспечения информационной безопасности.

УДК 004.056.5(076)
ББК 32.972.5я73

ISBN 978-985-543-587-8

© УО «Белорусский государственный
университет информатики
и радиоэлектроники», 2021

Библиотека БГУИР

СОДЕРЖАНИЕ

Библиотека БГУИР

ВВЕДЕНИЕ

Информация – один из критически важных факторов успеха деятельности любой организации. Необходимость защиты от внутренних угроз была очевидна на всех этапах развития средств информационной безопасности, но первоначально приоритет отдавался защите от угроз, связанных с внешними факторами. На сегодняшний день ситуация во многом изменилась, и с определенной уверенностью можно утверждать, что внутренние субъективные источники угроз безопасности информации, т. е. действия лиц, имеющих доступ к работе со штатными средствами вычислительной техники и (или) допуск в пределы контролируемой зоны, на практике столь же значимы, как и внешние [18].

Борьба с внутренними угрозами информационной безопасности представляет собой многогранную проблему. Технически утечка данных может произойти по множеству каналов: через корпоративный почтовый сервер, через интернет-канал при использовании публичных почтовых систем или веб-служб для размещения файлов, посредством беспроводных подключений (Wi-Fi, Bluetooth), принтера и мобильных носителей. Орудиями преступления могут стать фотокамеры, смартфоны, DVD, системы обмена мгновенными сообщениями (IM) и т. п. И несмотря на то, что эксперты все еще продолжают спорить о том, какие методы – технические или организационные – главенствуют при обеспечении внутренней безопасности, крупные отечественные и зарубежные компании уже достаточно давно инвестируют деньги в защиту данных, приобретая технические системы, предназначенные для предотвращения несанкционированного использования ключевой для бизнеса информации.

В настоящее время к современным средствам защиты информации, ориентированным на минимизацию внутренних угроз информационной безопасности, относят так называемые системы предотвращения утечки информации (Data Leak Prevention – DLP), внедряемые в целях выявления и блокирования нелегитимной передачи информации из защищенных автоматизированных систем [13]. К сожалению, детальный анализ DLP-решений затруднен по причине отсутствия нормативно-методической базы, регламентирующей требования к указанным системам. Тем не менее можно утверждать, что на сегодняшний день это один из наиболее эффективных инструментов для защиты конфиденциальной информации, и актуальность подобных решений будет со временем только увеличиваться.

Основными преимуществами DLP-систем перед альтернативными решениями (продуктами для шифрования, разграничения доступа, контроля доступа к сменным носителям, архивирования электронной корреспонденции, а также статистическими анализаторами) являются:

– наличие контроля всех регулярно используемых в повседневной деятельности каналов передачи конфиденциальной информации в электронном виде (включая локальные и сетевые способы);

Библиотека БГУИР

– обнаружение защищаемой информации по ее содержимому (независимо от формата хранения, каналов передачи, грифов и языка);

– блокирование утечек (приостановка отправки электронных сообщений или записи на USB-накопители, если эти действия противоречат принятой в компании политике безопасности);

– автоматизация обработки потоков информации согласно установленной политике безопасности (внедрение DLP-системы не требует расширения штата службы безопасности).

Следует отметить, что DLP-системы не могут в прямом смысле предотвратить ВСЕ утечки, поскольку существуют такие явления, как человеческий фактор, хакерские способы обхода системы защиты информации и т. п. В то же время коммерческая целесообразность рассматриваемых систем заключается в значительном снижении рисков утечки информации по неосторожности и в частичном снижении рисков преднамеренной кражи конфиденциальных сведений [1].

Библиотека БГУИР

1. ОБЩИЕ СВЕДЕНИЯ О DLP-СИСТЕМАХ

1.1. Назначение DLP-систем и принципы их функционирования

Что такое DLP применительно к информационной безопасности? Это комплекс технологий, позволяющих предотвратить утечку конфиденциальной информации. В течение последних нескольких лет для обозначения подобных систем использовалась достаточно разнообразная терминология: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) и др. Но окончательным и наиболее точным термином принято считать Data Leak Prevention (DLP), который был предложен аналитической компанией Forrester Research в 2005 г. [22]. В качестве русского аналога принято словосочетание «системы защиты конфиденциальных данных от внутренних угроз». При этом под внутренними угрозами подразумевают как умышленное, так и непреднамеренное злоупотребление сотрудниками своими правами доступа к данным.

DLP-система представляет собой комплекс программно-аппаратных средств, обеспечивающих защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента автоматизированной системы путем анализа и блокирования исходящего трафика.

Работа DLP-систем строится на перехвате и последующем анализе потоков данных, пересекающих периметр в направлении «вовне» либо циркулирующих внутри защищаемой корпоративной сети. Перехваченная информация анализируется с помощью различных поисковых алгоритмов, а при обнаружении данных, соответствующих выбранным критериям, срабатывает активная компонента системы, оповещая об инциденте сотрудника службы информационной безопасности (рис. 1.1).

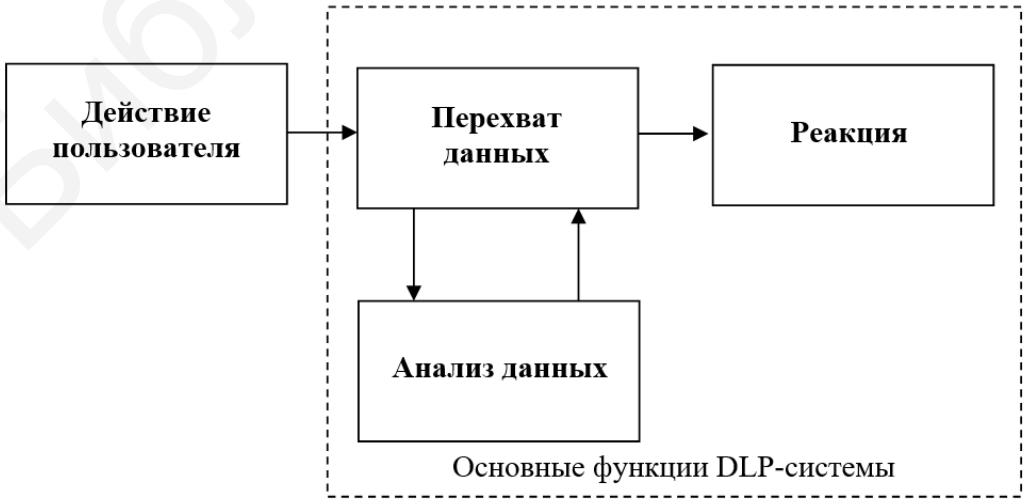


Рис. 1.1. Принцип функционирования DLP-системы

В ряде случаев передача сообщения (пакета, потока, сессии) может блокироваться. Существующие на данный момент DLP-системы обладают широкими функциональными возможностями и демонстрируют достаточно высокую эффективность при условии их грамотного применения [1].

DLP-системы можно условно разделить на три типа: системные (уровня хоста), сетевые и прикладные (как правило, уровня системы управления базами данных (СУБД)). Независимо от типов DLP-систем применяемые методы анализа данных бывают атрибутные (например, использующие свойства объектов системы) и семантические (основанные на смысловом анализе информации, как правило, путем выявления сочетаний ключевых данных).

Если говорить об истории развития DLP-технологий, то первыми появились технологии сетевого мониторинга без возможности блокировки утечки через сетевые протоколы (HTTP, SMTP и т. п.). В дальнейшем производители соответствующих решений стали добавлять функции блокировки информации при передаче данных через сеть.

Затем появилась возможность обеспечения контроля рабочих станций за счет внедрения на них программных «агентов», что позволило предотвращать передачу конфиденциальной информации с этих устройств (сюда же следует отнести контроль функций «copy/paste», снятия скриншотов, а также контроль передачи информации на уровне приложений, например, в одном приложении функций «copy/paste» разрешен, в другом – запрещен). И, наконец, появились технологии поиска конфиденциальной информации на сетевых ресурсах и ее защиты, в случае если данные обнаружены в тех местах, где их не должно быть. Конфиденциальная информация при этом задается предварительно ключевыми словами, словарями, регулярными выражениями, «цифровыми отпечатками» и т. п. В результате поиска система показывает, где она обнаружила конфиденциальную информацию, и какие политики безопасности при этом нарушаются. Затем сотрудник службы безопасности может принимать соответствующие меры. Есть решения, которые не просто показывают наличие конфиденциальной информации в неположенном месте, а переносят эту информацию «в карантин», оставляя в файле, в котором она была обнаружена, запись, куда перенесена информация и к кому обратиться за получением доступа к ней.

На текущий момент на рынке представлено довольно много DLP-решений, позволяющих выявлять и предотвращать утечки конфиденциальной информации по тем или иным каналам. При этом большинство корпоративных DLP-систем являются комплексными и включают следующие компоненты: модуль централизованного управления, клиентские агенты, модули анализа протоколов, модули сканирования (поиска) данных.

Библиотека БГУИР

1.2. Технические возможности получения информации об активности работников

С технической точки зрения существует несколько основных способов получения информации об активности работников. К ним относятся:

– системы идентификации и аутентификации;

– логирование (журналирование);

– перехват, мониторинг и анализ трафика.

Системы идентификации и аутентификации позволяют с высокой вероятностью определить подлинность пользователя либо удаленного узла. В общем случае они предназначены для однозначного определения субъекта доступа и его полномочий по отношению к конкретному ресурсу. Для описания соответствующих процедур используются понятия идентификации, аутентификации и авторизации.

Идентификация – это процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет системе свой идентификатор и она проверяет его наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными (законными), остальные – нелегальными.

Аутентификация – процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Для этого он должен подтвердить факт обладания определенной информацией, которая может быть доступна только ему одному (пароль, ключ и т. п.).

Авторизация – процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации, т. е. для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

На данный момент существуют следующие основные системы аутентификации пользователей:

– парольные (самый простой и распространенный способ);

– криптографические с открытым ключом / инфраструктура открытых ключей / криптографические сертификаты (системы PKI – Public Key Infrastructure);

– биометрические;

– системы одноразовых паролей.

Наиболее распространенным механизмом аутентификации пользователей является использование паролей и/или ответов на «секретный вопрос». Однако в силу сравнительно низкой криптостойкости и тех, и других соответствующие системы являются наиболее уязвимыми.

В простейшем случае системы идентификации и аутентификации позволяют осуществлять учет доступа работника как на ту или иную территорию, так и к определенным ресурсам. Примерами использования данного

Библиотека БГУИР

подхода являются смарт-карты, биометрические сканеры, пароли для учетных записей и другие подобные средства, являющиеся основой для построения так называемых систем контроля и управления доступом (СКУД). Информация в СКУД позволяет восстановить последовательность действий, которые совершал тот или иной работник. Недостаток подобных систем очевиден – они позволяют судить о характере деятельности человека лишь по косвенным критериям, не давая при этом полного представления о том, что делал человек непосредственно на своем рабочем месте.

Логирование (журналирование). Файл регистрации, протокол, журнал или лог (англ. log) – файл с записями о событиях в хронологическом порядке. Анализ различных логов позволяет получить более полную картину поведения работника. К примеру, анализ логов прокси-сервера покажет, какие ресурсы посещал сотрудник. На анализе логов строят свою деятельность системы Security Information and Event Management (SIEM), решающие задачи консолидации и хранения журналов событий от различных источников в сочетании с предоставлением инструментов для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам. SIEM-системы позволяют выявлять аномальное поведение и аномальную активность работников. К примеру, такая система может среагировать, если человек, который раньше работал исключительно с понедельника по пятницу, вдруг выйдет на работу в субботу или в воскресенье. Тем не менее у анализа логов тот же недостаток: сами по себе записи в логах являются лишь косвенным подтверждением предполагаемой активности работника; понять его намерения, опираясь на содержимое журналов, вряд ли получится.

Перехват, мониторинг и анализ трафика осуществляются при помощи так называемых снифферов. Сниффер (от англ. to sniff – нюхать) – сетевой анализатор трафика, т. е. программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа либо только анализа сетевого трафика, направляемого на другие узлы. Поскольку первоначально при использовании снифферов анализ трафика осуществлялся вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), изменялась возможность анализа лишь небольших его объемов. Сегодня снифферы, как правило, включаются в состав более сложных систем, обладающих развитыми аналитическими функциями. Именно к таким и относятся рассматриваемые DLP-системы. Перехват трафика позволяет максимально полно контролировать работника, так как помимо анализа косвенных признаков (посещаемые ресурсы, действия с файлами и т. д.) появляется и прямая информация о действиях человека: содержание переписки по электронной почте, переписки при помощи систем обмена мгновенными сообщениями (Instant Messaging – IM), снимки рабочего стола и другие сведения.

Библиотека БГУИР

1.3. Виды перехвата информации

В настоящее время чаще всего используются следующие способы перехвата информации:

– перехват в разрыв;

– сетевой перехват;

– перехват путем интеграции со сторонними продуктами;

– агентский перехват.

Перехват в разрыв. В этом случае весь трафик компании пропускается через специальное физическое устройство. На сегодняшний день такой вид перехвата не пользуется большой популярностью у производителей DLP-систем, так как при его применении слишком велики угрозы бизнесу. В случае отказа/«падения» подобного устройства в компании автоматически останавливается практически все информационные потоки.

Сетевой перехват. Данный подход основан на том, что большое число существующих управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов на отдельно взятый порт. В основном эта функция применяется для мониторинга трафика в целях обеспечения его безопасности либо для оценки производительности/загрузки сетевого оборудования с применением аппаратных средств, но также может быть использована и для работы DLP-системы. В этом случае весь сетевой трафик направляется на коммутатор с поддержкой функции «зеркалирования» (англ. mirroring) портов. Коммутатор снимает с трафика копию, которая, в свою очередь, затем анализируется.

Преимущества способа сетевого перехвата:

– независимость от операционной системы компьютера работника;

– отсутствие дополнительной нагрузки на сеть;

– незаметность для работников и антивирусных программ.

Недостатки способа сетевого перехвата:

– проблемы с перехватом шифрованного трафика;

– малое количество контролируемых каналов.

Перехват путем интеграции со сторонними продуктами. Этот вид перехвата ориентирован на работу с прокси-серверами и почтовыми серверами, имеет незначительные отличия от сетевого перехвата. Главное из них заключается в том, что вместо адреса сетевого адаптера, с которого будет «сниматься» трафик, указываются сервер и порт подключения к нему. Применительно к интеграции, например, с почтовым сервером, схема работы выглядит так:

– на почтовом сервере настраивается ящик, в который сервер складывает абсолютно всю почту (и входящую, и исходящую);

– DLP-система периодически опрашивает этот ящик и забирает оттуда письма; период опроса, как правило, может настраиваться произвольно;

– после «выемки» почты осуществляется очистка ящика, чтобы там не накапливались письма.

Библиотека БГУИР

Главное преимущество перехвата путем интеграции с почтовыми серверами заключается в возможности перехвата почтовых сообщений, передаваемых по шифрованному каналу. Главный недостаток – еще меньшее количество контролируемых каналов в сравнении с сетевым перехватом.

Агентский перехват. В общем случае агенты представляют собой сервисы/программы, устанавливаемые непосредственно на компьютер или планшет пользователя и предназначенные для перехвата информации, а также ее дальнейшей отсылки на сервер для анализа.

Этот вид перехвата на сегодняшний день пользуется наибольшим вниманием производителей DLP-систем и обладает рядом несомненных достоинств.

Преимущества способа агентского перехвата:

– контроль всех каналов информации;

– осуществление перехвата шифрованного трафика;

– в случае необходимости блокировка передачи информации.

Недостатки способа агентского перехвата:

– дополнительная (сравнительно небольшая) нагрузка на сеть;

– необходимость присутствия агента непосредственно на компьютере работника;

– потребность в отдельных агентах для каждой операционной системы.

1.4. Состав и взаимосвязь компонентов DLP-систем на примере программного комплекса «Контур информационной безопасности SearchInform»

DLP-система «Контур информационной безопасности SearchInform» (далее – КИБ) предназначена для выявления и предотвращения утечек конфиденциальной информации и персональных данных, а также обнаружения фактов наличия конфиденциальной информации на компьютерах сотрудников и нерационального использования ими рабочего времени [11].

КИБ построен на основе клиент-серверной архитектуры. Под серверными компонентами подразумеваются платформы перехвата данных SearchInform-NetworkSniffer и SearchInformEndpointSniffer [4, 5], под клиентскими – приложения, предназначенные для поиска и просмотра перехваченных данных в целях проведения служебных расследований [2, 6]. Наличие единого поискового аналитического движка позволяет в полной мере использовать имеющиеся поисковые возможности.

Компоненты КИБ обеспечивают перехват, сохранение и анализ всех данных, передаваемых пользователем по контролируемым каналам передачи информации. Перехват данных осуществляется сервером NetworkSniffer либо агентами EndpointSniffer, установленными на целевые рабочие станции пользователей. Функциональная схема КИБ представлена на рис. 1.2.

Библиотека БГУИР

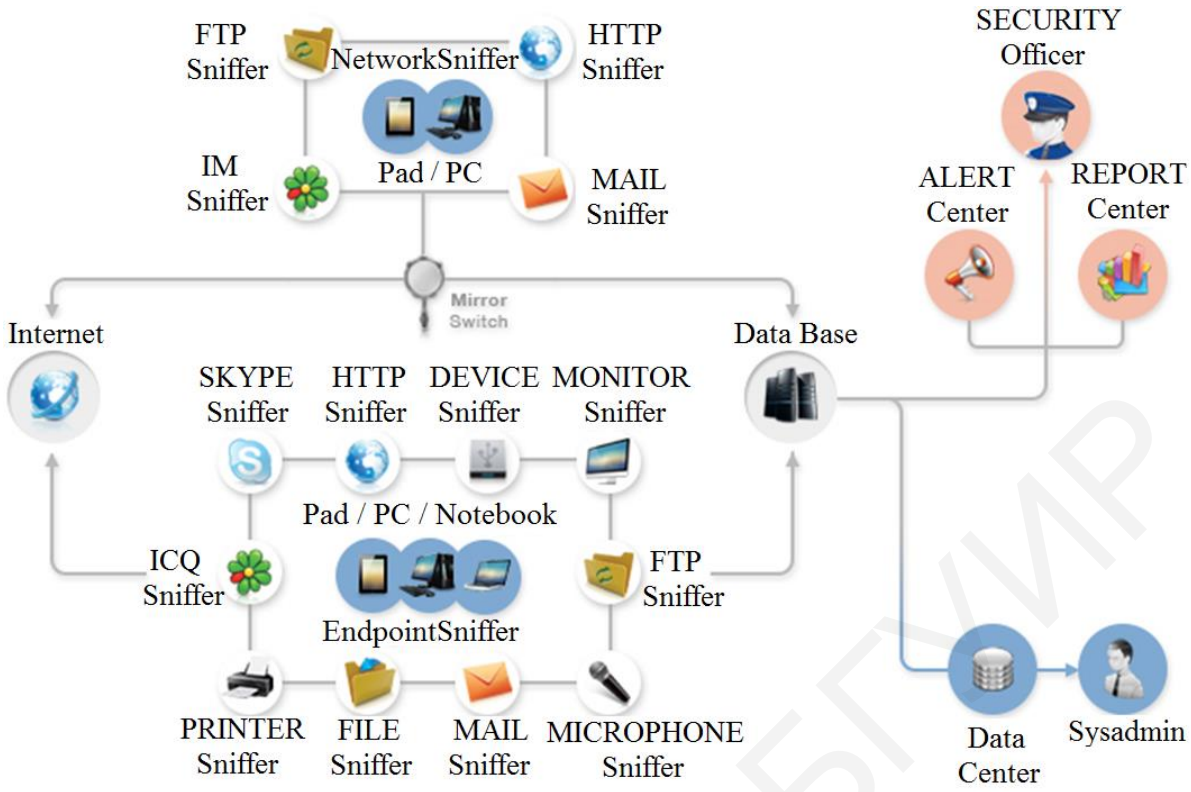


Рис. 1.2. Функциональная схема КИБ

Взаимодействие основных компонентов КИБ осуществляется следующим образом.

Сервер NetworkSniffer анализирует сетевой трафик на уровне TCP/IP-пакетов и осуществляет выделение контролируемой информации в трафике, идентификацию пользователей, а также сохранение результата перехвата в базы данных; поддерживает перехват данных для следующих компонентов: MailSniffer, IMSniffer, HTTPSniffer, FTPSniffer.

Агенты EndpointSniffer устанавливаются на рабочие станции пользователей и перехватывают документы пользователей непосредственно на рабочих станциях; поддерживают перехват данных для следующих компонентов: SkypeSniffer, DeviceSniffer, PrintSniffer, MonitorSniffer, FileSniffer, HTTPSniffer, FTPSniffer, IMSniffer, MailSniffer, MicrophoneSniffer, KeyloggerSniffer, ProgramSniffer, LyncSniffer. Также агент EndpointSniffer может устанавливаться на мобильное устройство на базе iOS и осуществлять перехват данных, отправляемых/получаемых пользователем мобильного устройства (продукт MobileSniffer).

Агенты передают данные не напрямую в базу или хранилище, а через серверы управления. Так, например, агент MobileSniffer, установленный на мобильное устройство, перехватывает и передает данные по VPN-каналу, агент VPN-сервера передает перехваченную информацию серверу EndpointSniffer.

Сервер SoftInform Search с помощью специализированных агентов обеспечивает проведение индексации рабочих станций (ИРС), за счет чего

становится возможным выявление конфиденциальной информации на жестких дисках пользователей. Агенты ИРС не помещают документы в базу данных, а ведут локальные протоколы файловой системы на рабочих станциях пользователей.

Перехваченная информация помещается в базы данных SQL или файловое хранилище. В частности, серверы NetworkSniffer (компоненты MailSniffer, IMSniffer, HTTPSniffer) и EndpointSniffer (компоненты SkypeSniffer, PrintSniffer, MailSniffer, MonitorSniffer, FileSniffer, MicrophoneSniffer, HTTP-Sniffer, IMSniffer, KeyloggerSniffer, LyncSniffer, ProgramSniffer, MobileSniffer) помещают перехваченные сообщения и файлы в базы данных, а компоненты FTPSniffer и DeviceSniffer используют для перехваченных данных хранилище.

Поскольку базы данных, хранилища и файлы на жестких дисках рабочих станций не обеспечивают быстрый доступ к данным, то для повышения производительности системы перехваченные документы индексируются. Индекс – структура, обеспечивающая быстрый поиск по тексту и формальным признакам перехваченных документов.

Для управления индексами и базами данных (далее – БД) компонентов предназначен продукт DataCenter. Известно, что по мере роста объема данных снижается скорость работы SQL-сервера и замедляется выполнение поисковых запросов, поэтому базы данных и индексы рекомендуется разбивать. DataCenter позволяет задать условия, по достижении которых будет автоматически создаваться новый индекс или база данных с настроенным перехватом. Также SearchInform DataCenter контролирует факт поступления перехватываемых данных в индексы и базы данных, работу компонентов КИБ, наличие свободного дискового пространства для работы системы и, в зависимости от настроек, извещает пользователя о различных событиях или неудовлетворительных условиях для функционирования системы.

Созданные индексы предоставляют следующие возможности поиска по перехваченным документам:

а) полнотекстовый поиск – вид поиска по ключевым словам и словосочетаниям в тексте перехваченных документов, при котором не учитывается порядок слов и их положение в документе;

б) фразовый поиск – вид поиска по ключевым словам с учетом их положения друг относительно друга, позволяющий отсечь документы, в которых ключевые слова разбросаны по всему тексту;

в) «поиск похожих» – вид поиска, при реализации которого используется запрос, представляющий собой целый текст, с которым сравнивается каждый перехваченный документ;

г) поиск по словарю – вид поиска, позволяющий отыскать документы, относящиеся к определенной тематике: все документы в индексе проверяются на наличие в них содержимого из указанного тематического словаря;

д) атрибутный поиск – поиск по атрибутам перехваченных документов, таким как дата/время перехвата, имя компьютера, имя пользователя домена, IP/MAC-адрес и др.

Для поиска по индексам и базам данных перехваченных документов используется поисковый клиент SearchInform Client.

Проверка перехваченных данных автоматизируется при помощи клиент-серверного компонента AlertCenter, который позволяет:

а) настраивать политики информационной безопасности, задавать для них поисковые запросы, используемые для выявления конфиденциальных данных во всех контролируемых потоках информации (почта, Skype, службы мгновенных сообщений, социальные сети и форумы, печать и внешние носители, FTP-соединения и др.);

б) регистрировать пользователей, от имени которых будет осуществляться доступ к серверу баз данных Microsoft SQL Server, а также аудиторов службы безопасности, которые будут получать уведомления AlertCenter. Для каждого из таких пользователей дополнительно можно настроить права доступа относительно каждой созданной политики безопасности: только ее просмотр, право изменения либо запрет доступа как к самой политике, так и к результатам проверки по ней;

в) хранить все настройки и журнал инцидентов в базе данных под управлением Microsoft SQL Server;

г) настраивать политики карантина;

д) настраивать уведомления об инцидентах;

е) просматривать журнал инцидентов;

ж) открывать документы, по которым зафиксированы инциденты, в клиентских приложениях КИБ и в сопоставленных приложениях.

Продукт SearchInform ReportCenter позволяет формировать статистику по активности пользователей и фактам нарушения политик информационной безопасности (инцидентам), представляя статистические данные в виде отчетов. Предоставляемые ReportCenter данные – емкий по содержанию и хорошо оформленный материал, который может использоваться для служебных отчетов отдела безопасности компании и оказать неоценимую помощь при проведении служебных расследований.

Общая схема работы КИБ представлена на рис. 1.3. Как правило, для нормального функционирования КИБ достаточно двух-трех физических/виртуальных серверов, но в тех случаях, когда требуется высокая производительность, каждый серверный компонент может быть установлен на отдельный сервер.

Библиотека БГУИР

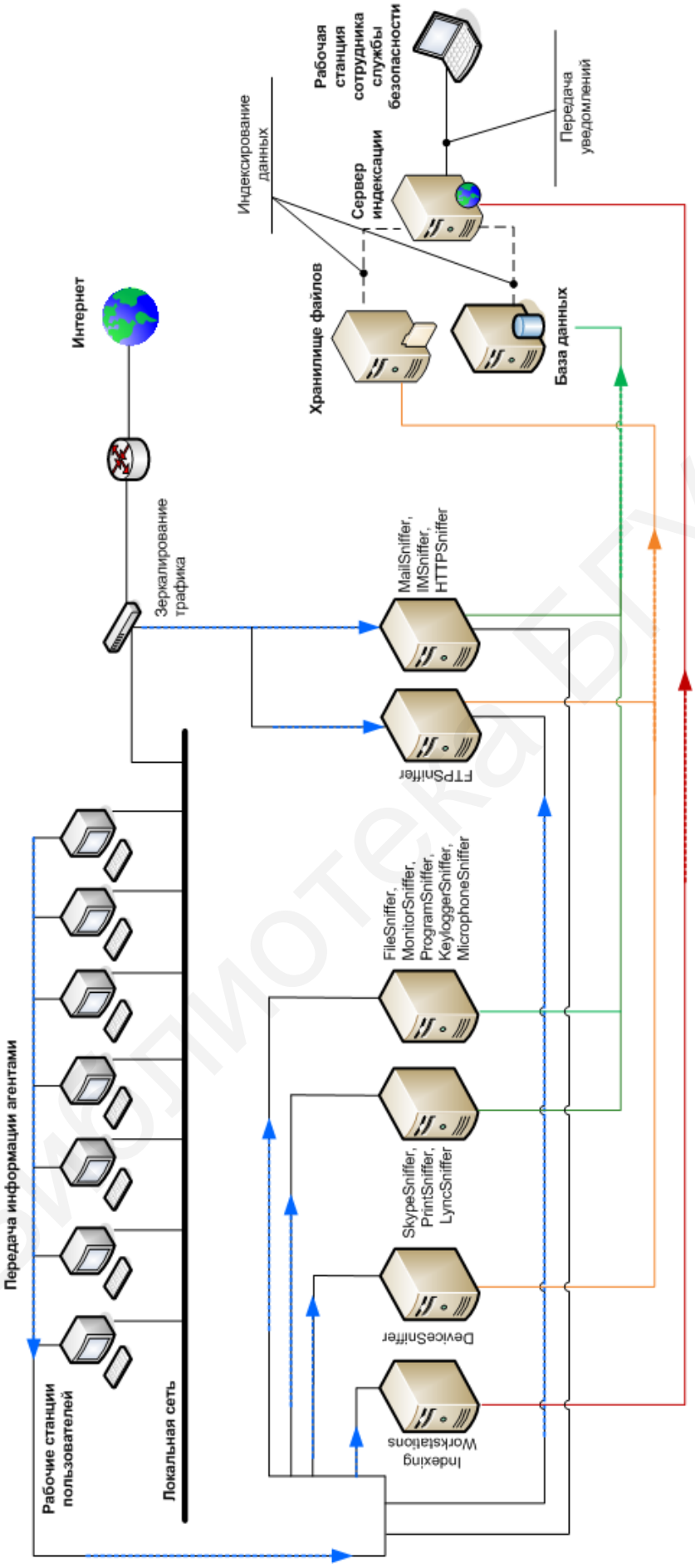


Рис. 1.3. Общая схема работы КИБ

Библиотека БГУИР

2. СЕРВЕРНЫЕ КОМПОНЕНТЫ ПРОГРАММНОГО КОМПЛЕКСА «КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM»

2.1. Платформа SearchInform NetworkSniffer: особенности реализации сетевого перехвата трафика

Общая характеристика и принцип работы SearchInform NetworkSniffer [5]. Платформа SearchInform NetworkSniffer предназначена для перехвата сетевого трафика, извлечения из него сообщений и файлов, записи в базу данных и поиска по ней. Трафик перехватывается в точке сети, через которую проходит сетевой трафик, и чаще всего перенаправляется при помощи устройства (например, сетевого маршрутизатора), поддерживающего зеркалирование сетевых пакетов.

SearchInform NetworkSniffer обрабатывает трафик, не оказывая влияния на работу корпоративной сети, и позволяет осуществлять перехват данных, пересылаемых пользователями по таким сетевым протоколам, как SMTP, POP3, HTTP(S), IMAP, MAPI, NNTP, ICQ, XMPP, MMP, MSN, YAHOO, SIP, Gadu-Gadu, FTP и Cloud. Схематичное изображение работы рассматриваемой платформы представлено на рис. 2.1.

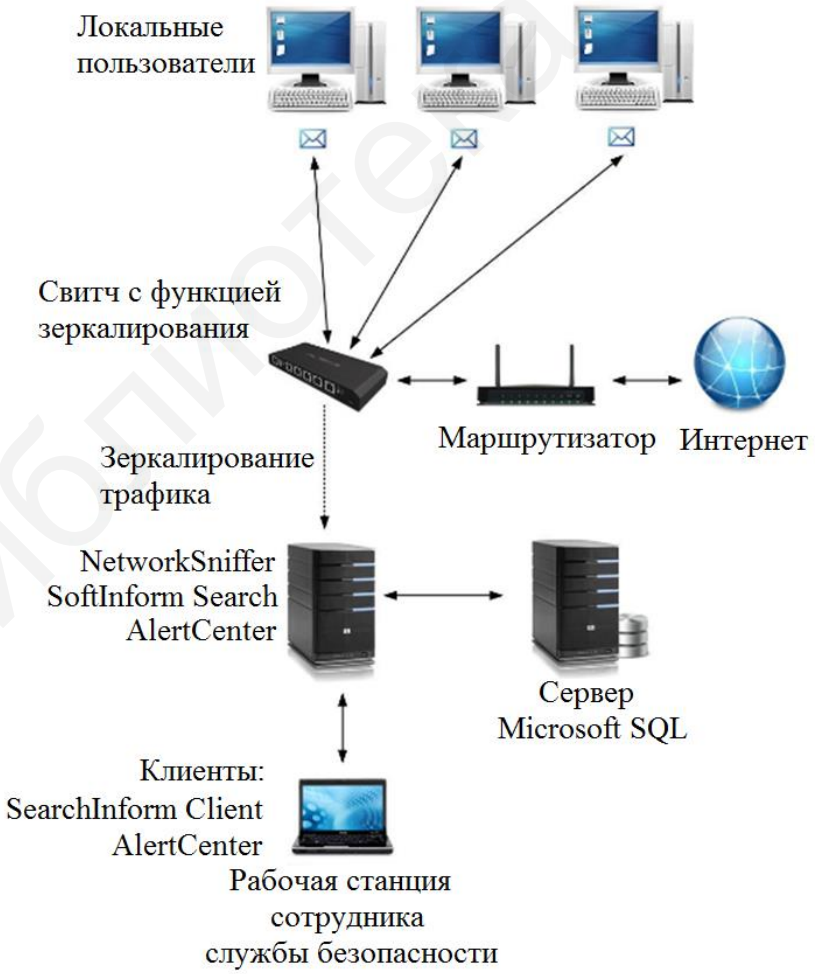


Рис. 2.1. Схема работы SearchInform NetworkSniffer

Библиотека БГУИР

Перехват сетевого трафика производится на уровне сетевых протоколов (Mail, HTTP, IM, FTP). Возможна фильтрация по доменному имени пользователя, имени компьютера, IP- и MAC-адресам. Перехваченные сообщения помещаются в базу данных SQL, которая индексируется при помощи SoftInform SearchServer. Индекс представляет собой особую структуру, необходимую для осуществления быстрого поиска по содержимому перехваченных документов.

При помощи приложения SearchInform AlertCenter данные того или иного индекса с заданным интервалом проверяются на соответствие заранее настроенным политикам безопасности, состоящим из поисковых запросов. Расписание проверок и список запросов настраиваются работниками службы безопасности организации. В случае обнаружения совпадений SearchInform AlertCenter немедленно оповещает об этом сотрудника службы безопасности.

Консоль администратора SearchInform NetworkSniffer. Управление серверной частью платформы осуществляется при помощи консоли.

Основной способ мониторинга интернет-трафика – прослушивание трафика в точке, через которую проходят сетевые пакеты. Чаще всего трафик перенаправляется на сервер NetworkSniffer при помощи шлюза с функцией зеркалирования сетевых пакетов. Это может быть сетевой концентратор (хаб), маршрутизатор (роутер), коммутатор (свитч) или другое устройство. Настройка параметров сетевого перехвата производится в узле настроек «Сетевой перехват» (рис. 2.2).

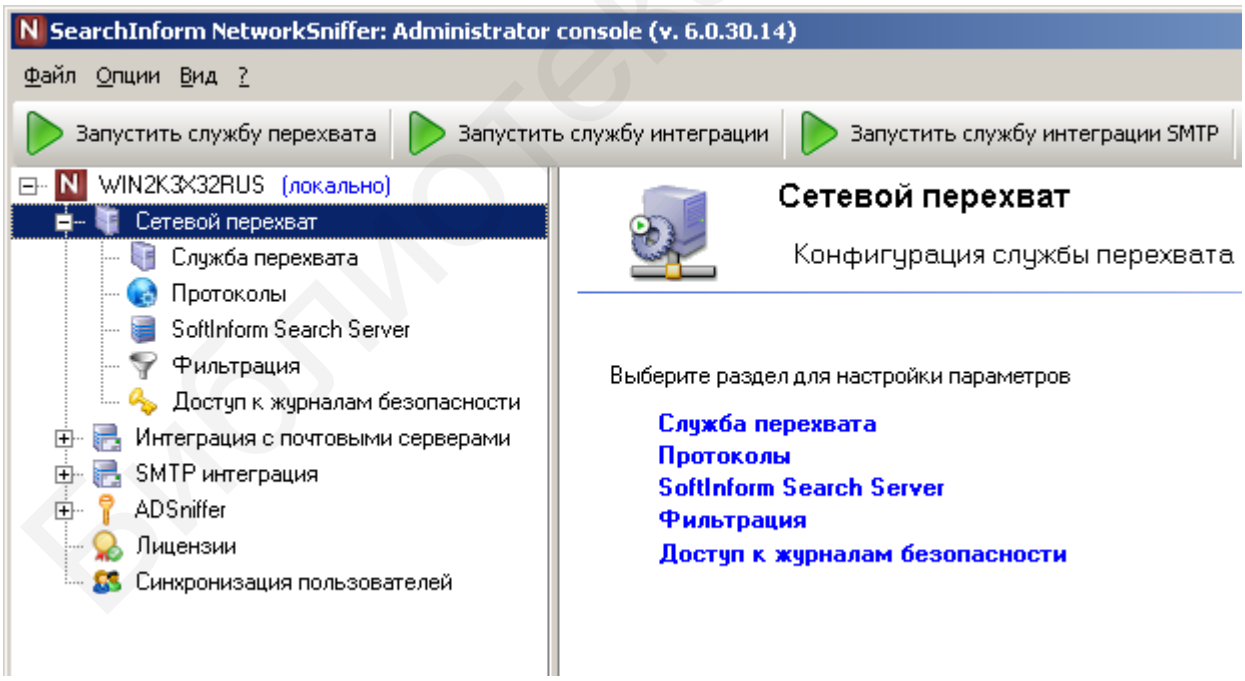


Рис. 2.2. Узел настроек «Сетевой перехват»

Служба перехвата. В этом разделе осуществляются настройки типа запуска службы перехвата, уровня логирования и управления сетевыми адаптерами (рис. 2.3).

Библиотека БГУИР

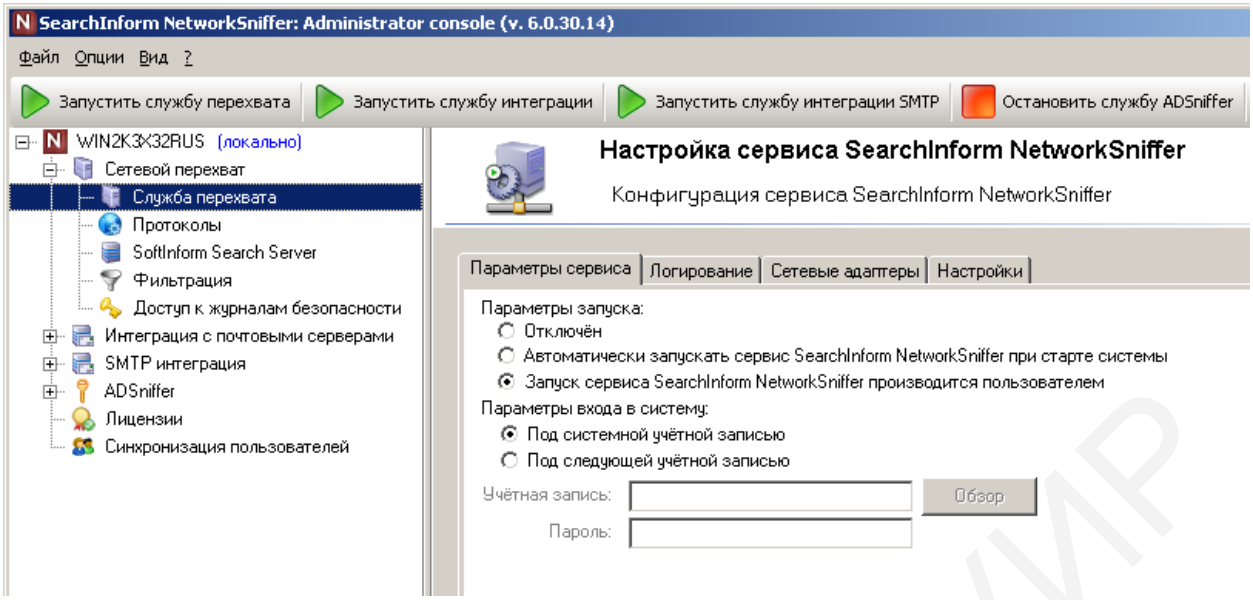


Рис. 2.3. Настройка службы перехвата

Возможны следующие типы запуска службы перехвата: «Отключен» (будучи активизированной, данная настройка не разрешает перезапуск службы перехвата), «Автоматически при старте системы» и «Запуск производится пользователем».

При этом следует помнить, что для получения доменных имен пользователей учетная запись, под которой работает служба перехвата, должна иметь права чтения журналов безопасности. Системная учетная запись обычно не обладает данными правами. Поэтому для настройки учетной записи следует выбрать опцию «Под следующей учетной записью», после чего ввести имя и пароль пользователя с правами чтения журналов безопасности.

В диагностических целях может потребоваться изменение настроек протоколирования работы службы перехвата. Доступны следующие уровни логирования:

– «обычный» – фиксируются серьезные ошибки службы синхронизации и консоли управления сервером, повлекшие прерывание или аварийное завершение работы, а также факты запуска внутренних функций программы;

– «детальный» – дополнительно фиксируется запуск внутренних функций программы в подробном виде; данный режим рекомендуется включать только по запросу сотрудников службы технической поддержки в случае проблем с программным обеспечением.

Сетевые пакеты, которые нужно подвергать мониторингу, могут поступать на один или несколько физических или виртуальных сетевых адаптеров сервера NetworkSniffer. Поэтому для осуществления перехвата должны быть выбраны соответствующие сетевые адаптеры. Настройка списка сетевых адаптеров осуществляется на вкладке «Сетевые адаптеры» (рис. 2.4).

Библиотека БГУИР

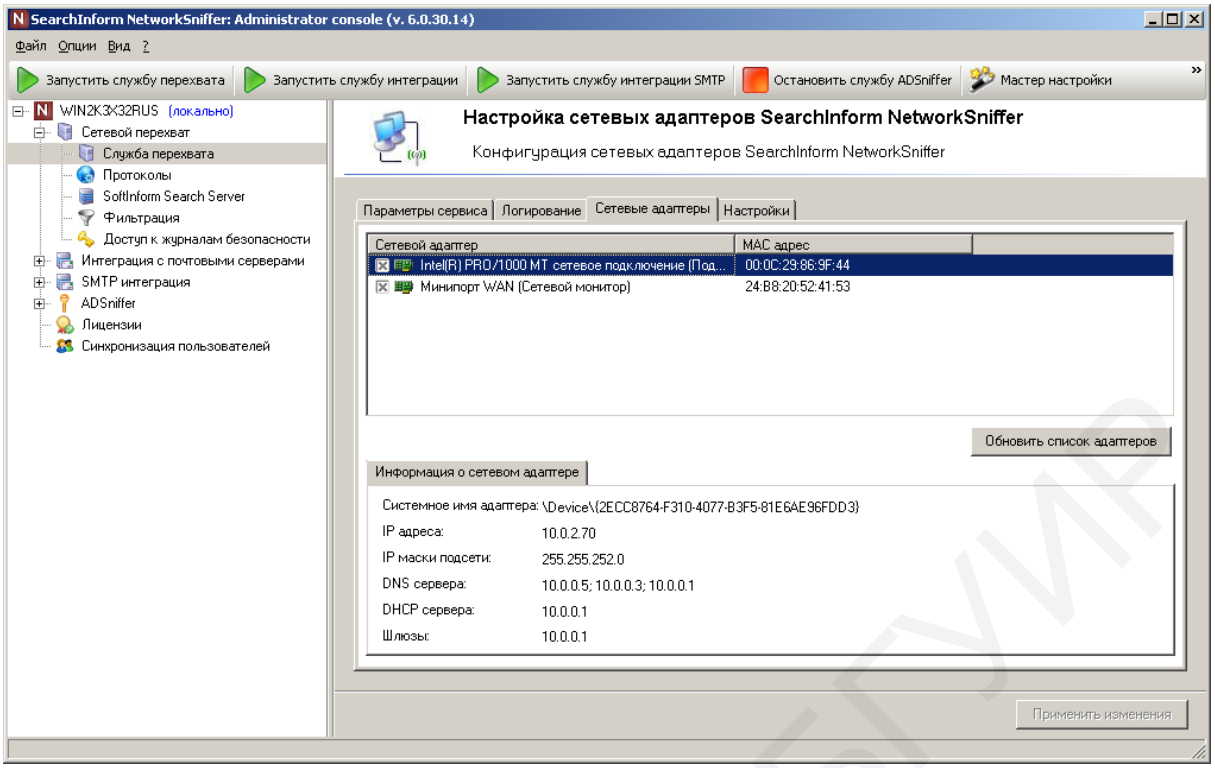


Рис. 2.4. Выбор сетевого адаптера

На правой верхней панели отображается список доступных аппаратных и программных сетевых интерфейсов, из числа которых необходимо указать сетевые или виртуальные устройства, на которые, в свою очередь, поступает трафик. Для предотвращения потери пакетов в настройках отмеченных сетевых карт должны быть отключены все offload-параметры. Рекомендуется включать перехват только с тех устройств, на которые поступает сетевой трафик, так как для прослушивания каждого адаптера используются дополнительные системные ресурсы. Ограничив список адаптеров, можно повысить производительность системы в целом.

Зачастую в списке адаптеров сетевого перехвата присутствует WAN Miniport. Его следует использовать, когда NetworkSniffer получает данные от сервера ISA/TMG (в режиме интеграции).

В этом случае флажком отмечается только WAN-порт, поскольку консоль требует, чтобы перехват был включен хотя бы на одном адаптере. С реальных сетевых карт флажки должны быть сняты. В остальных ситуациях перехват трафика с WAN-порта не требуется. Для взаимодействия NetworkSniffer с программными и аппаратными прокси-серверами, работающими по протоколу ICAP, необходимо произвести следующие настройки:

1) на вкладке «Настройки» включить протокол ICAP, установив флажок в строке «ICAP»;

2) указать IP-адрес сервера NetworkSniffer, который будет выступать в качестве ICAP-сервера; прокси-сервер в данном случае должен быть настроен как ICAP-клиент;

3) указать прослушиваемый ICAP-сервером порт.

Библиотека БГУИР

Протоколы. Изначально трафик представляет собой «смесь» пакетов данных, передаваемых при помощи различных протоколов. Это происходит потому, что работники одновременно используют и электронную почту, и интернет-браузер, и Skype, и другие средства коммуникации. Поэтому следующим шагом в работе является использование так называемых протоколов парсеров. Их задача – разложить информацию «по полочкам» в SQL-базы. Данная операция выполняется при первой настройке DLP-системы «Контур информационной безопасности SearchInform». Для каждого протокола можно задать свою собственную базу данных, но можно и сгруппировать их, к примеру, все почтовые протоколы складывать в одну базу, все протоколы IM – в другую. Кроме того, для каждого протокола можно задать порт или диапазон портов, которыми будет ограничен перехват. В противном случае трафик будет собираться со всех доступных портов.

Как уже было сказано, для корректной работы NetworkSniffer каждый обрабатываемый протокол должен быть привязан к базе данных (хранилищу), в которую(-ое) записываются сообщения и файлы. NetworkSniffer поддерживает управление базами данных при помощи следующих СУБД:

– Microsoft SQL Server 2005+;

– PostgreSQL 8.3+;

– SQLite (рекомендуется использовать только при тестировании NetworkSniffer).

Привязка протокола к базе данных/хранилищу производится в узле «Протоколы» (рис. 2.5). Для привязки протокола к базе данных или хранилищу необходимо выделить требуемый протокол, нажать кнопку «Настроить хранилище данных», расположенную на вкладке «Информация о протоколе», и настроить подключение к новой или уже существующей базе или файловому хранилищу. Протоколы, к которым не привязаны базы данных, отмечаются полужирным шрифтом.

Некоторые протоколы являются совместимыми. Это значит, что к одной базе можно привязать несколько совместимых протоколов, но можно использовать и отдельные базы данных. NetworkSniffer может перехватывать данные различных типов:

– почтовые сообщения и вложенные файлы;

– сообщения и файлы IM-клиентов;

– данные, передаваемые при помощи веб-форм (HTTP (POST)-запросы), а также GET-запросы поисковых систем;

– файлы, передаваемые или принимаемые по FTP-протоколу;

– данные, передаваемые при помощи облачных хранилищ.

Данные этих типов имеют различный формат и характеризуются особыми формальными признаками. Например, почтовым сообщениям обычно присвоены значения почтовых адресов отправителя и получателя, тема сообщения, а IM-сообщениям – значения UIN и псевдонимов. Соответственно данные, различающиеся своим форматом, записываются в базы разной конфигурации, с различным набором таблиц и ячеек. В то же время,

Библиотека БГУИР

если формальные признаки позволяют перехваченные данные отнести к одному типу, становится возможным использование базы данных одной конфигурации. Данные о совместимости протоколов представлены в табл. 2.1.

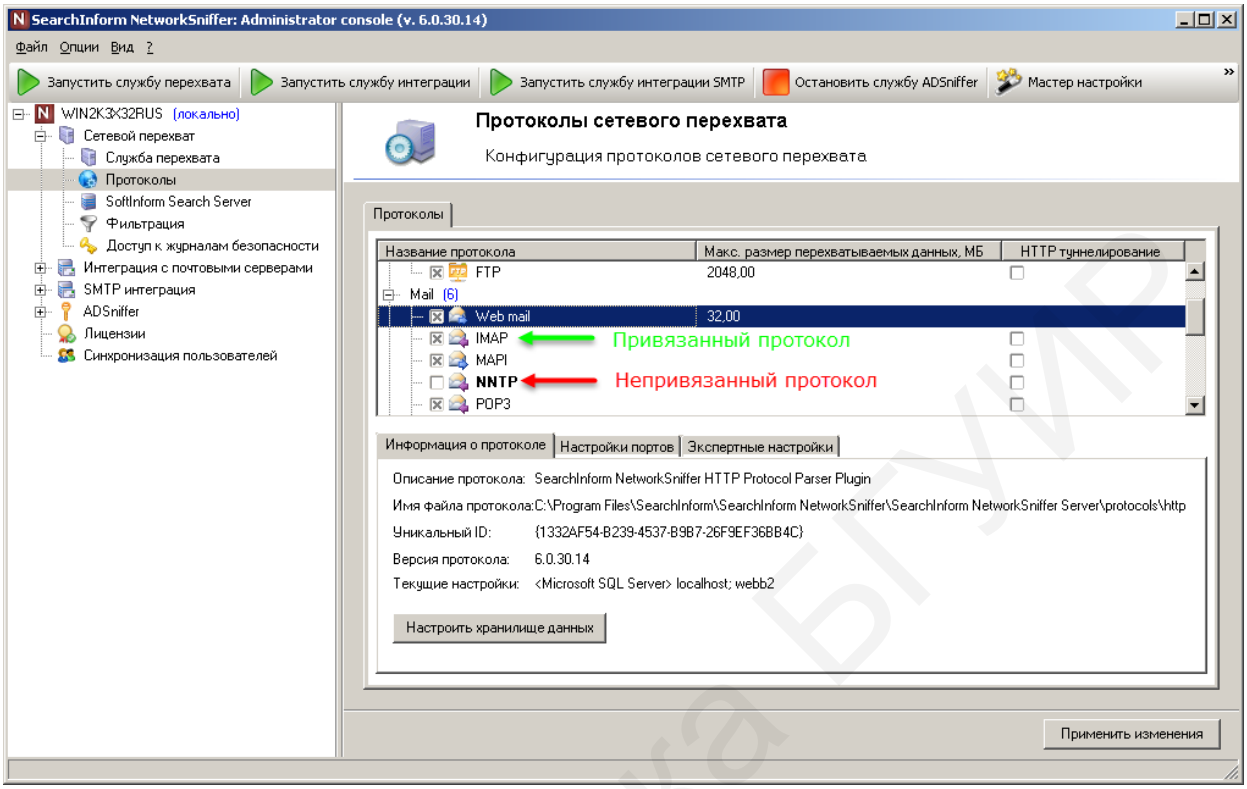


Рис. 2.5. Привязка протокола к базе данных или хранилищу

Таблица 2.1

Совместимость протоколов

Совместимые почтовые протоколы	**Совместимые IM-протоколы**	**HTTP (POST)-запросы**	**FTP-протокол**	**CLOUD**
Web mail IMAP MAPI POP3 SMTP NNTP	HTTP IM MMP MSN ICQ XMPP SIP	HTTP POST	FTP	Cloud & SharePoint

Также каждый обрабатываемый протокол должен быть привязан к портам, через которые передается информация. Если известны сетевые порты, которые используются конкретным протоколом, рекомендуется ограничивать прослушивание портов для этого протокола, что может повысить общую производительность системы. По умолчанию сервер NetworkSniffer обрабатывает трафик с ограниченного числа портов:

– WEB MAIL / HTTP POST / HTTP IM / CLOUD – 80;
– IMAP – 143;
– MAPI – 1118;
– NNTP – 119 (NNTPS – 563);

Библиотека БГУИР

– MMP – 443;
– MSN – 1863;
– ICQ – 443;
– SIP – 5060;
– POP3 – 110;
– SMTP – 25;
– XMPP – 5222;
– FTP – 21.

Тем не менее трафик может «проходить» и через другие порты. Например, для передачи почтовых сообщений по протоколу SMTP часто используется порт 2525, почтовый сервер mail.ru использует SMTP-порт 587, а при передаче сообщений ICQ по HTTP-туннелю может быть задействован порт 80. В таких случаях к протоколу нужно привязать новые порты.

Для привязки протоколов к портам необходимо в узле «Протоколы» в группе «Сетевой перехват» выделить требуемый протокол и открыть вкладку «Настройки портов» (рис. 2.6). При установленном флажке в строке «Ограничить перехват трафика указанными портами» NetworkSniffer анализирует сетевые пакеты только по заданному диапазону портов. Если флажок снят, протокол NetworkSniffer анализирует сетевые пакеты, полученные со всех портов.

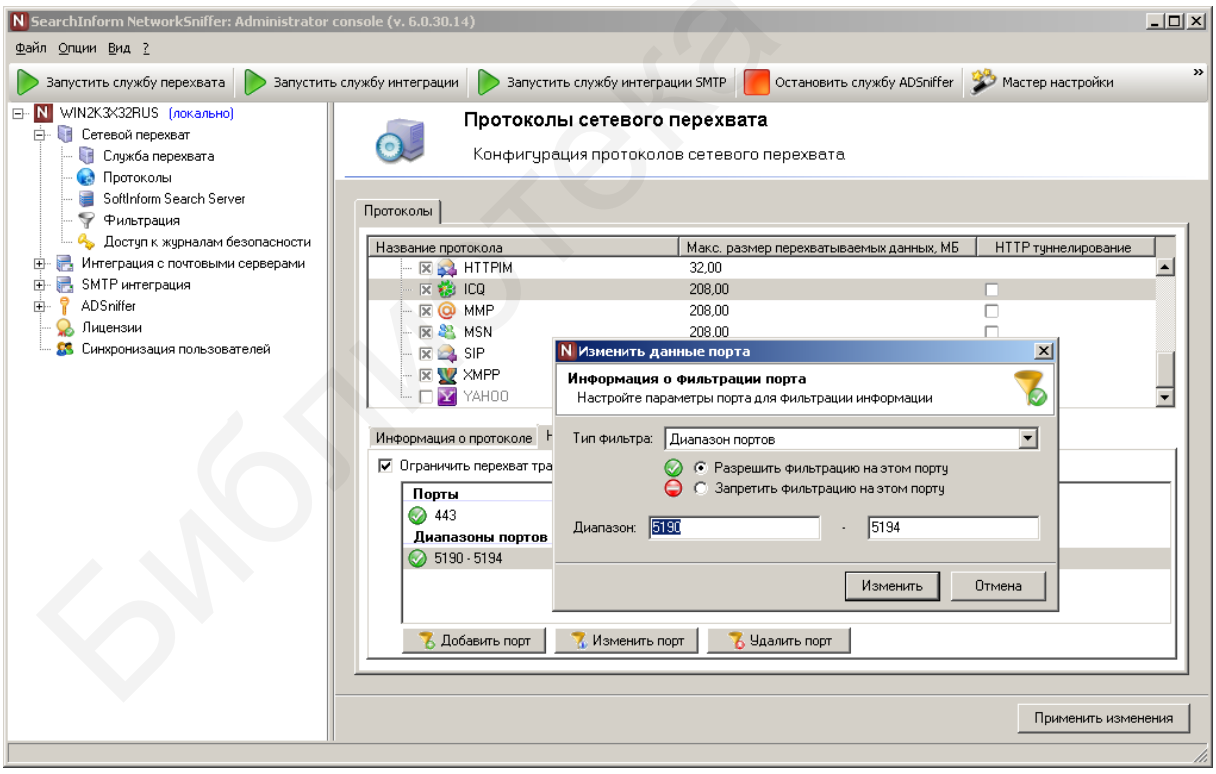


Рис. 2.6. Привязка протоколов к портам

Привязка протоколов к портам осуществляется при помощи кнопок «Добавить порт», «Удалить порт», «Изменить порт».

Система перехвата трафика строит «карту сетевых портов» и привязывает к каждому порту конкретный протокол. Например, если для протокола

PROTOCOL1 настроен порт 1090, а для протокола PROTOCOL2 – перехват со всех портов, то для порта 1090 в карте будет соответствовать PROTOCOL1 и PROTOCOL2. В этом случае все сетевые пакеты, в которых присутствует данный номер порта, будут направляться для обработки в оба модуля разбора протоколов (парсера).

Очень часто в локальных сетях устанавливаются прокси-серверы, которые разрешают передачу/получение данных в Интернете только по протоколу HTTP. Для передачи данных по другим протоколам в таких сетях может использоваться HTTP-туннелирование.

Туннелирование – это организация передачи данных одного протокола через другой. Соответственно HTTP-туннелирование подразумевает передачу в рамках HTTP-протокола данных других протоколов. В этом случае данные другого протокола «оборачиваются» в HTTP-заголовки и таким образом могут быть переданы через прокси-сервер, разрешающий передачу данных только по протоколу HTTP. В качестве примера можно привести IM-клиент Pidgin, который позволяет настроить передачу информации в службу MSN по HTTP-туннелю.

Перехват туннелированного трафика активизируется путем выбора требуемого протокола и установки флажка  в столбце HTTP-туннелирование. При задействовании данной функции нагрузка на сервер NetworkSniffer возрастает, поэтому рекомендуется использовать ее только в случае подозрения на неполный перехват сообщений и только для IM-протоколов.

При этом если порты, через которые идет туннелированный трафик, неизвестны, следует снять флажок в строке «Ограничить перехват трафика указанными портами», т. к. переданная по HTTP-туннелю информация не обязательно идет через стандартный HTTP-порт. Если же порты, через которые идет туннелированный трафик, известны (например, есть прокси-сервер с открытым портом 80), следует ввести порт или диапазон портов.

В NetworkSniffer входят различные модули разбора протоколов, используемые для перехвата HTTP-трафика (отправка данных через окно браузера):

– WEB MAIL (перехват входящих/исходящих почтовых сообщений с сервисов веб-почты);

– HTTP POST (перехват данных, отправляемых в блоги, форумы, чаты при помощи веб-форм (метод POST), а также запросы поисковых систем (метод GET));

– HTTP IM (перехват отправленных и полученных сообщений в социальных сетях, основанный на перехвате данных, передаваемых по протоколу HTTP).

Формат данных, отправляемых по HTTP-протоколу, может изменяться в зависимости от сайта, специфики отправляемых данных и целого ряда иных факторов. Поэтому может потребоваться дополнительная настройка параметров разбора трафика по данным протоколам.

Библиотека БГУИР

Сервер NetworkSniffer позволяет перехватывать сообщения веб-почты, отправляемые пользователями сети через окно браузера. В комплект поставки NetworkSniffer включены фильтры для перехвата сообщений, отправляемых с некоторых почтовых хостов. В дополнение к этому можно настроить функцию автораспознавания новых хостов веб-почты.

Для вызова диалогового окна настройки фильтра по почтовым хостам следует выделить Web mail в списке включенных протоколов, перейти на вкладку «Экспертные настройки» и нажать кнопку «Настройка» (рис. 2.7).

В открывшемся диалоговом окне (рис. 2.8) необходимо установить флажок в строке «Автоматический разбор сообщений», а если при просмотре почтового ящика с помощью браузера помимо исходящих электронных писем требуется перехватывать также входящие данные, то и флажок в строке «Перехват входящей почты». Кнопка «Применить» позволяет задействовать сделанные настройки.

Анонимайзеры позволяют перемещаться по любым сайтам, не выдавая истинного IP-адреса. Анонимайзер может быть программой, устанавливаемой на компьютер, или специальным веб-сайтом (веб-прокси). Для добавления в список анонимайзера необходимо нажать кнопку «Добавить» и в диалоговом окне «Новый анонимайзер» ввести требуемое значение (рис. 2.9).

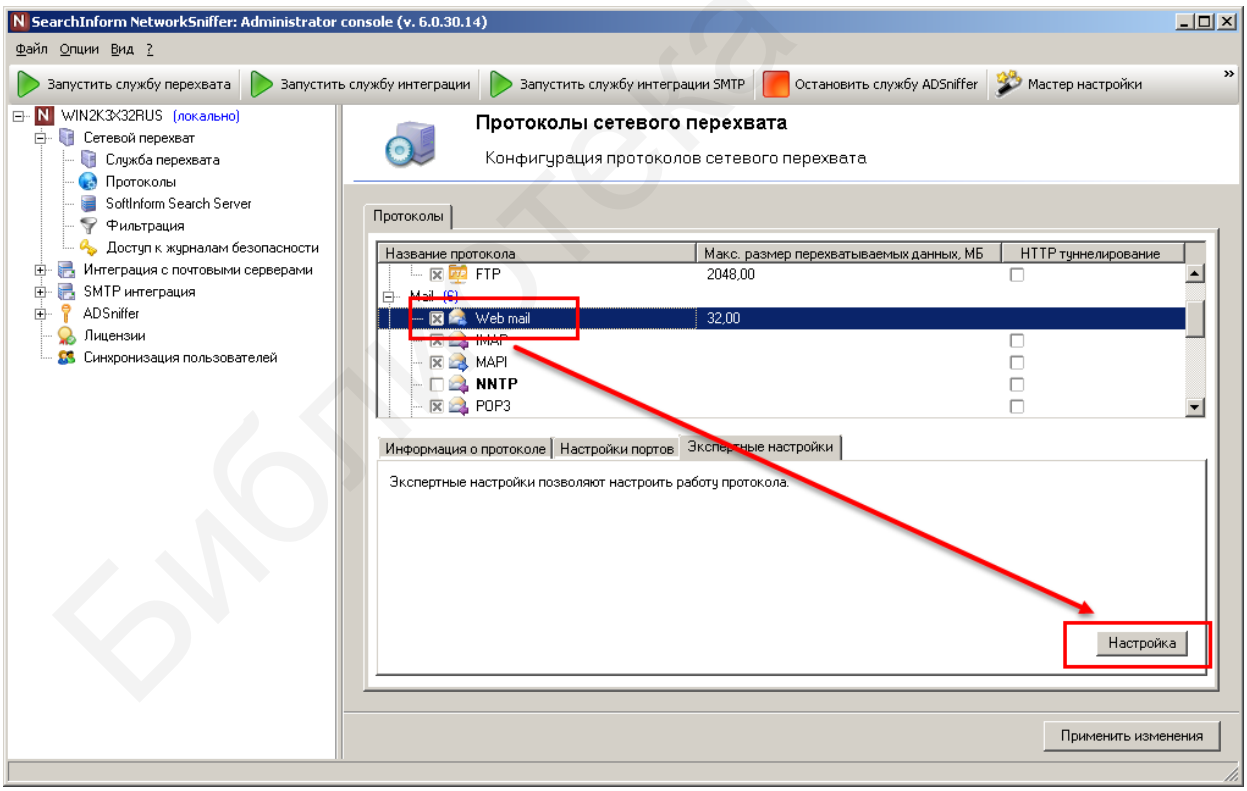


Рис. 2.7. Переход к экспертным настройкам Web mail

Библиотека БГУИР

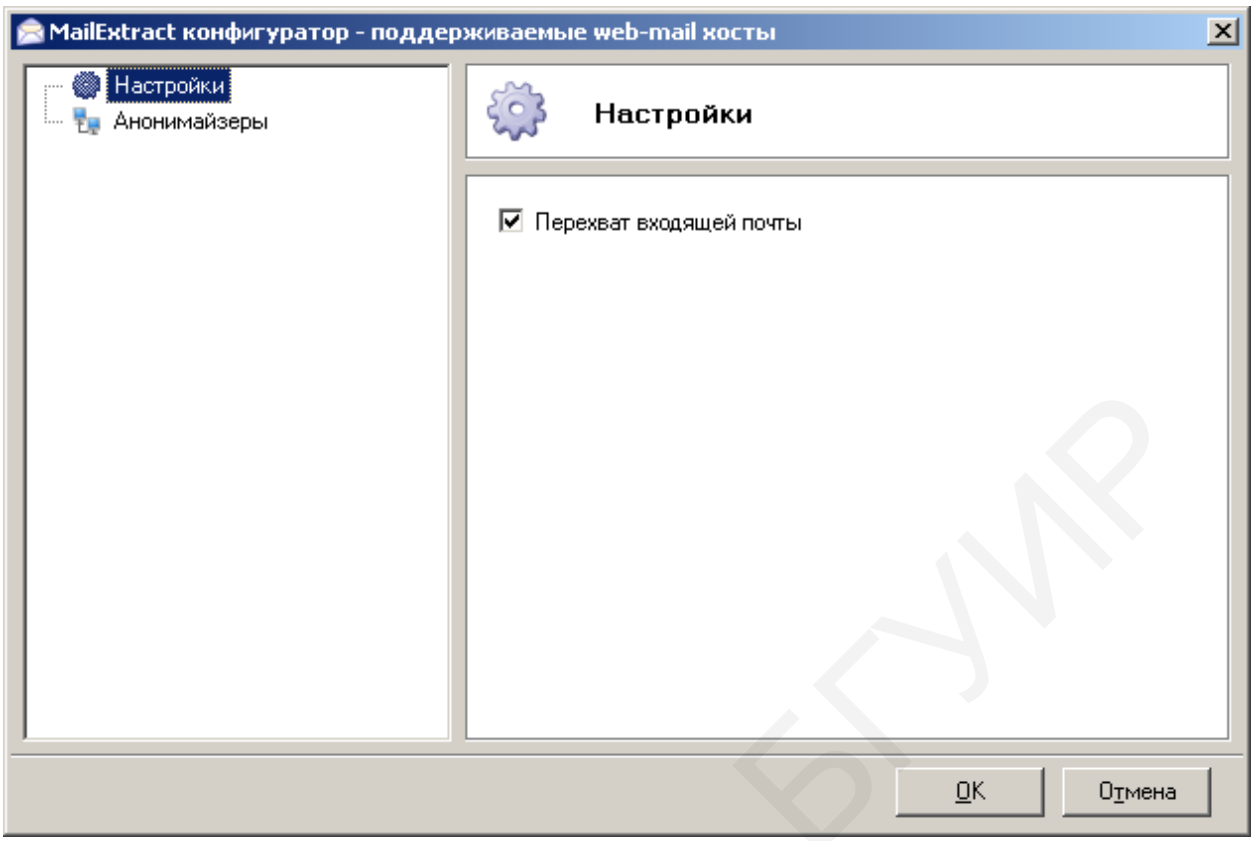


Рис. 2.8. Диалоговое окно настройки фильтра по почтовым хостам

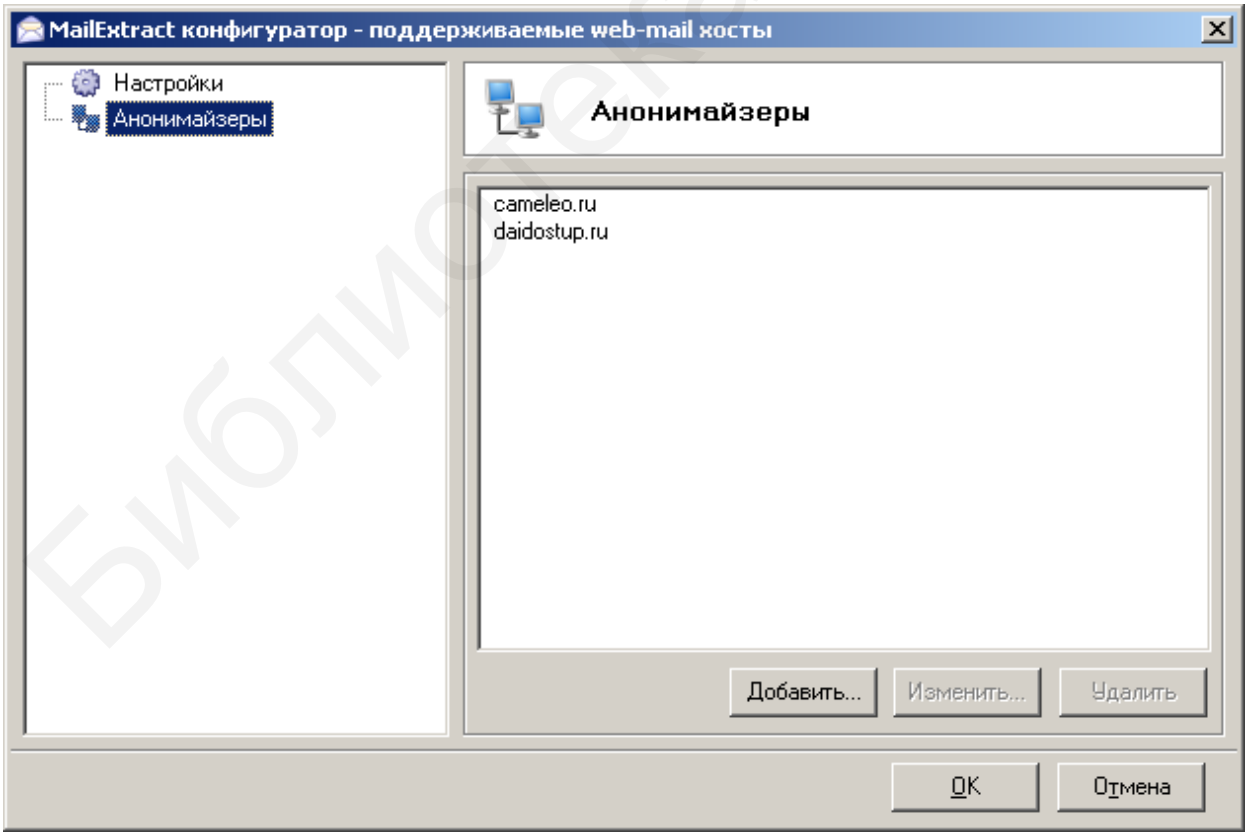


Рис. 2.9. Добавление анонимайзера

Библиотека БГУИР

Для просмотра настроек обработки протокола HTTP (POST) следует выделить HTTP (POST) в списке протоколов и нажать кнопку «Настройка» на вкладке «Экспертные настройки». В окне настроек протокола можно задать минимальный размер перехваченных данных (рис. 2.10).

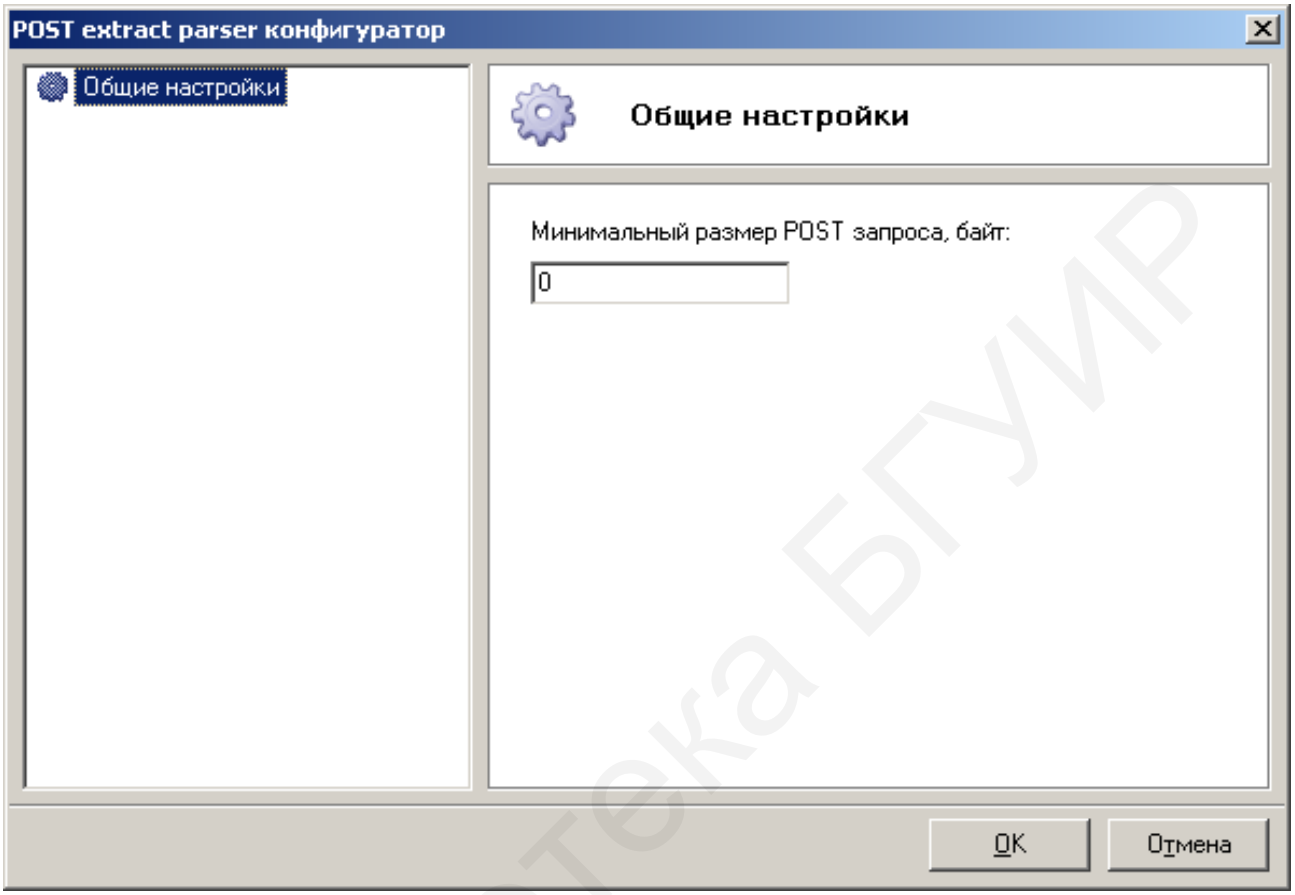


Рис. 2.10. Настройки обработки протокола HTTP (POST)

В дополнение к обработке POST-запросов, служащих для передачи информации в блоги, форумы, социальные сети и другие службы, сервер NetworkSniffer позволяет перехватывать GET-запросы, специфика которых заключается в том, что информация содержится не в передаваемых пакетах, а в строке URL-адреса. Чаще всего GET-запросы используются поисковыми службами, например, Google, Яндекс, Рамблер. Сервер NetworkSniffer перехватывает URL-адреса страниц, посещаемых пользователями, извлекает поисковые запросы и записывает их в привязанную к протоколу HTTP (POST) базу данных.

Сервер NetworkSniffer позволяет перехватывать отправленные и полученные сообщения социальных сетей. В настоящий момент поддерживается перехват в следующих социальных сетях: Одноклассники, Facebook, ВКонтакте, МойМир@Mail.ru, LinkedIn, Google+, Мамба, Imo.im, Meebo.com.

Для просмотра настроек обработки протокола HTTP IM следует выделить позицию HTTPIM в списке протоколов и нажать кнопку «Настройка» на вкладке «Экспертные настройки» (рис. 2.11).

Библиотека БГУИР

Анонимайзеры позволяют пользоваться социальными сетями даже в том случае, когда системный администратор блокирует доступ к таким доменам. В данном случае, чтобы произвести парсинг (разбор трафика) перехваченных сообщений, необходимо ввести список используемых пользователями анонимайзеров (аналогично тому, как это было рассмотрено для экспертных настроек Web mail).

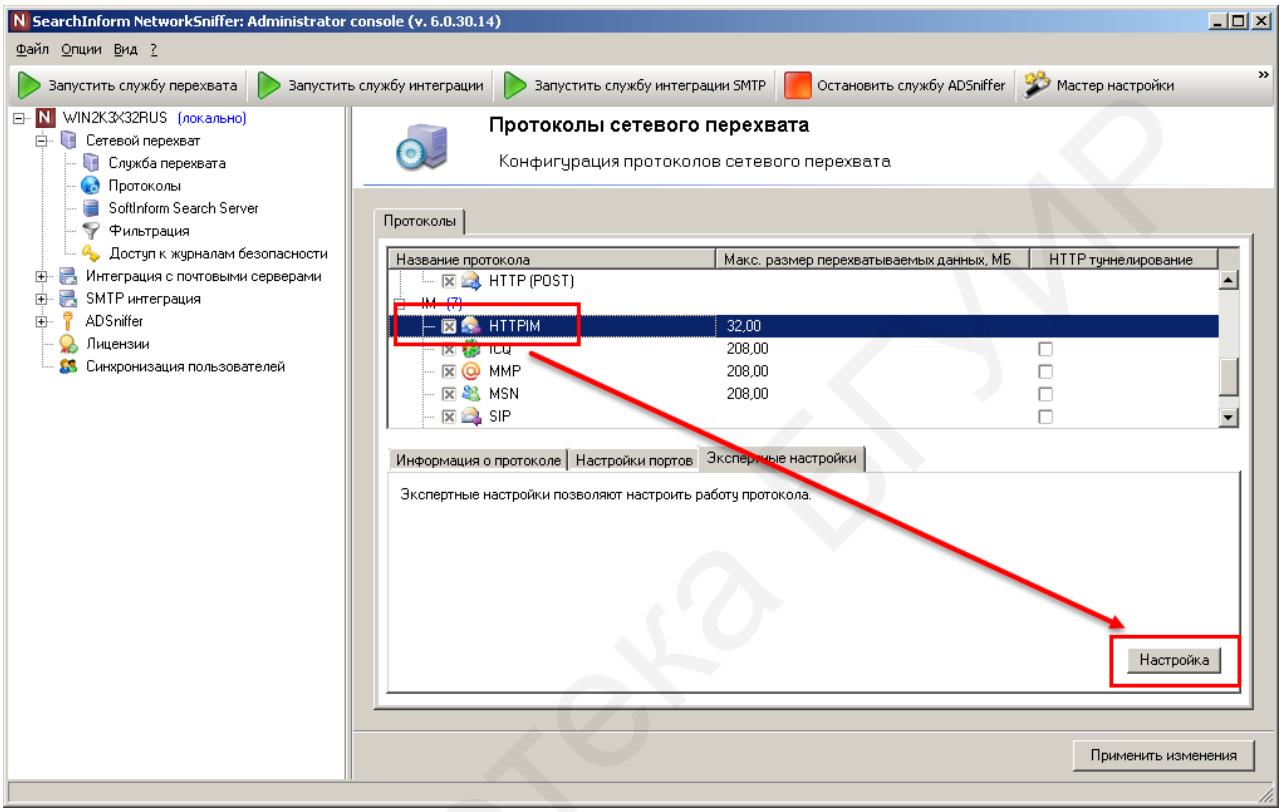


Рис. 2.11. Настройки обработки протокола HTTP IM

Сервер NetworkSniffer позволяет перехватывать и данные, передаваемые по протоколу SIP с помощью программных телефонов (например, X-Lite).

Для просмотра настроек перехвата протокола SIP необходимо выделить SIP в списке протоколов и нажать кнопку «Настройка» на вкладке «Экспертные настройки». Для перехвата голосовых сеансов связи помимо текстовых, следует установить флажок в строке «Перехват звонков» (рис. 2.12).

SoftInform Search Server. Поиск по перехваченным данным и их анализ производится через индексы поисковой подсистемы. Для осуществления операций с индексами локально или в сети должен быть установлен сервер SoftInform Search. С помощью консоли NetworkSniffer можно создавать только индексы протоколов, запись которых в базу данных производится самим сервером.

Настройка индексов данных, перехваченных в точке, через которую проходят сетевые пакеты, производится на вкладке «SoftInform Search Server» группы узлов «Сетевой перехват», а также из окна «Мастер быстрой настройки».

Библиотека БГУИР

Запуск/остановка сервера SoftInform Search производится путем нажатия кнопки «Запустить сервер»/«Остановить сервер» (в зависимости от его текущего состояния) (рис. 2.13).

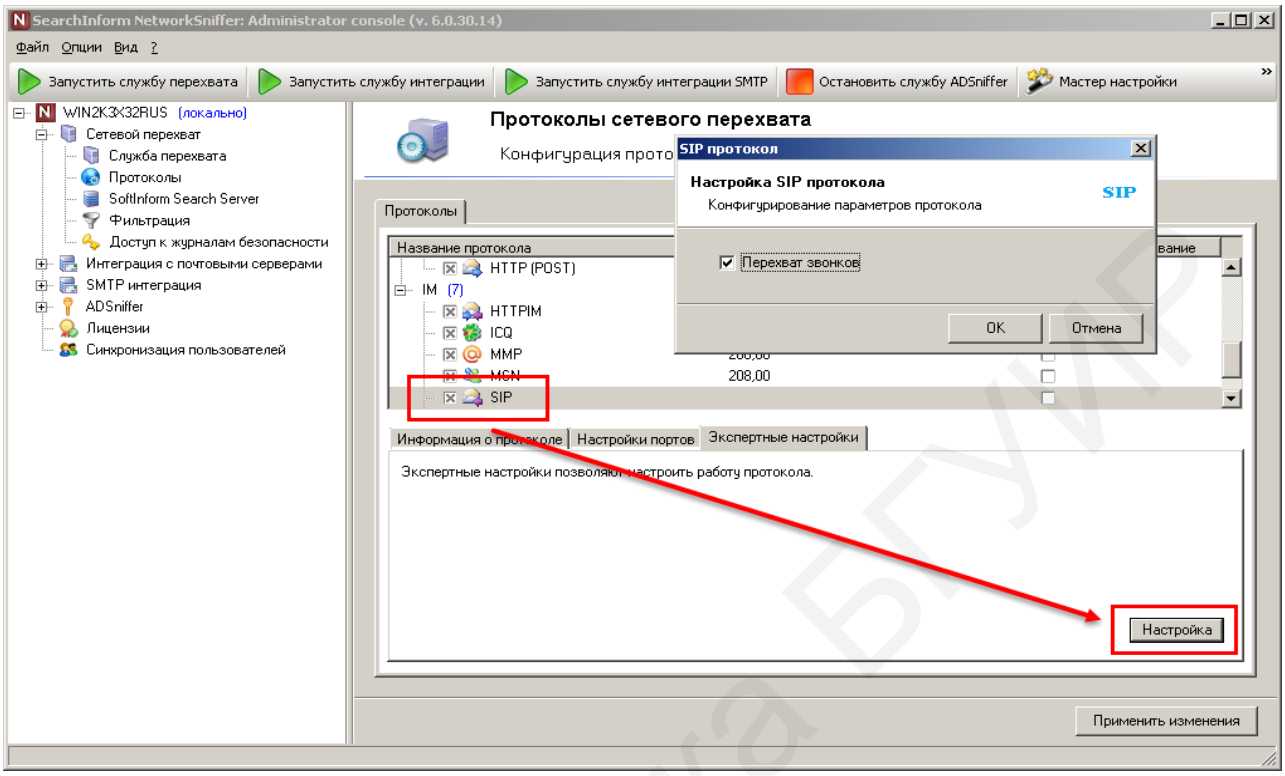


Рис. 2.12. Настройки обработки протокола SIP

Стандартные операции с индексами, которые могут быть осуществлены в консоли администратора SearchInform NetworkSniffer:

– создание индекса;

– обновление индекса по расписанию или вручную;

– очистка и удаление индекса;

– добавление и удаление источников данных;

– подключение существующего индекса.

Создание индексов производится либо из консоли администрирования NetworkSniffer, либо из серверной консоли SoftInform Search.

Тем не менее для создания новых индексов рекомендуется использовать консоль сервера NetworkSniffer, т. к. в этом случае происходит привязка баз данных к активному протоколу (сервер NetworkSniffer сохраняет новые перехваченные сообщения и файлы в указанную базу данных). Создавать индексы из консоли сервера SoftInform Search следует только для баз, которые больше не будут использоваться для записи новых документов.

Библиотека БГУИР

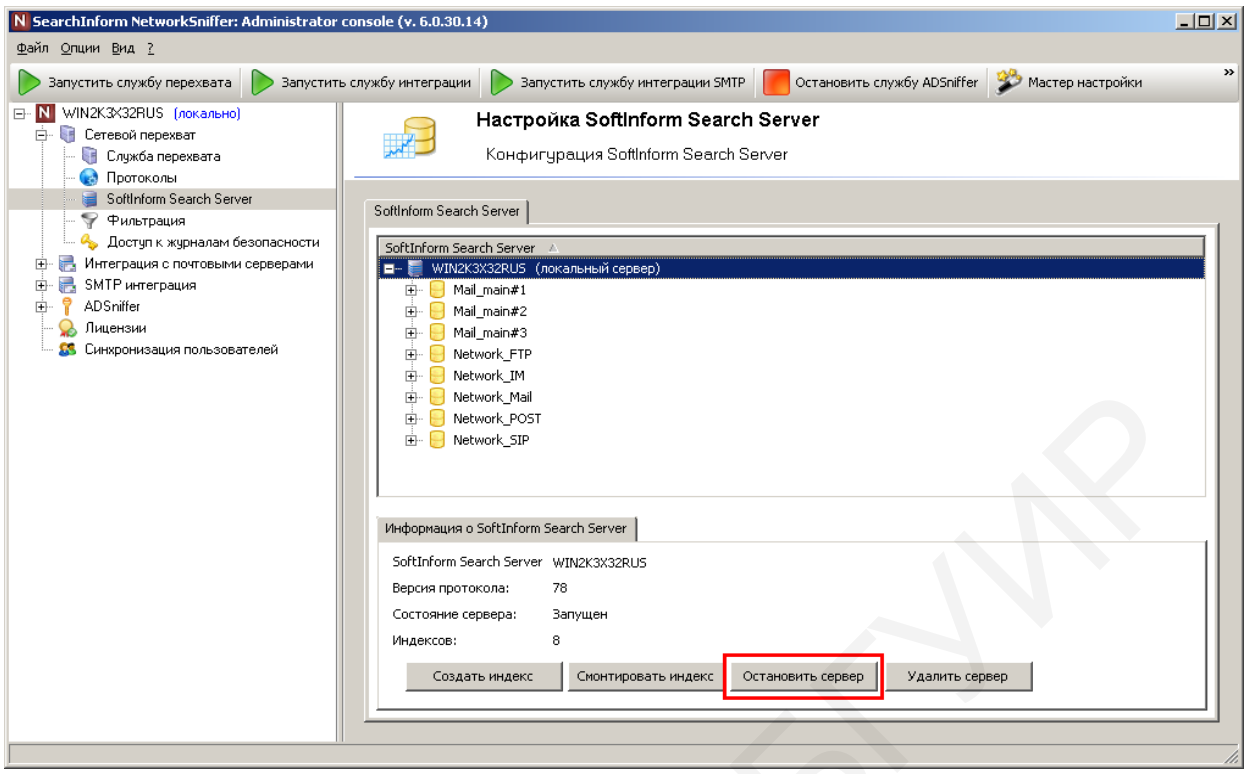


Рис. 2.13. Запуск/остановка сервера SoftInform Search

Для создания индекса предназначена кнопка «Создать индекс». При помощи мастера следует выполнить следующие шаги:

– выбрать сервер SoftInform Search или ввести его имя/IP-адрес, а также указать, к чему создается подключение (к базе данных или хранилищу файлов);

– при подключении к БД выбрать тип СУБД – Microsoft SQL Server, PostgreSQL или SQLite (используется только в рамках тестирования), после чего настроить подключение к базе данных (создать новую или подключиться к уже существующей);

– при подключении к хранилищу файлов в диалоговом окне «Настройка источника данных» вручную либо с помощью кнопки  выбрать/создать *.sti-файл для хранения перехваченных данных; при создании нового каталога подтвердить запрос на его создание;

– выбрать протоколы данных, включенных в индекс (при этом NetworkSniffer будет складывать сообщения, перехваченные по указанным протоколам, в подключенную БД (хранилище)), затем установить флажок в строке «Автоматически запускать перехват»;

– в завершение создания индекса ввести имя индекса и выбрать директорию, по которой индекс будет храниться.

Новый индекс будет отображен в консоли NetworkSniffer. Для созданного индекса рекомендуется настроить расписание обновления.

Запуск обновления индекса возможен как в автоматическом режиме (по расписанию), так и вручную. Для настройки автоматического обновления индекса необходимо воспользоваться планировщиком. Для этого следует выде-

Библиотека БГУИР

лить индекс и открыть вкладку «Планировщик». Имеющаяся там кнопка «Добавить расписание» открывает окно «Мастер создания расписания», кнопка «Изменить расписание» – окно «Мастер редактирования расписания», а кнопка «Удалить расписание» позволяет удалить выделенное расписание.

Для обновления данных, содержащихся в выделенном индексе, необходимо вручную перейти на вкладку «Свойства индекса» и, предварительно выделив индекс, нажать кнопку «Начать обновление» (рис. 2.14).

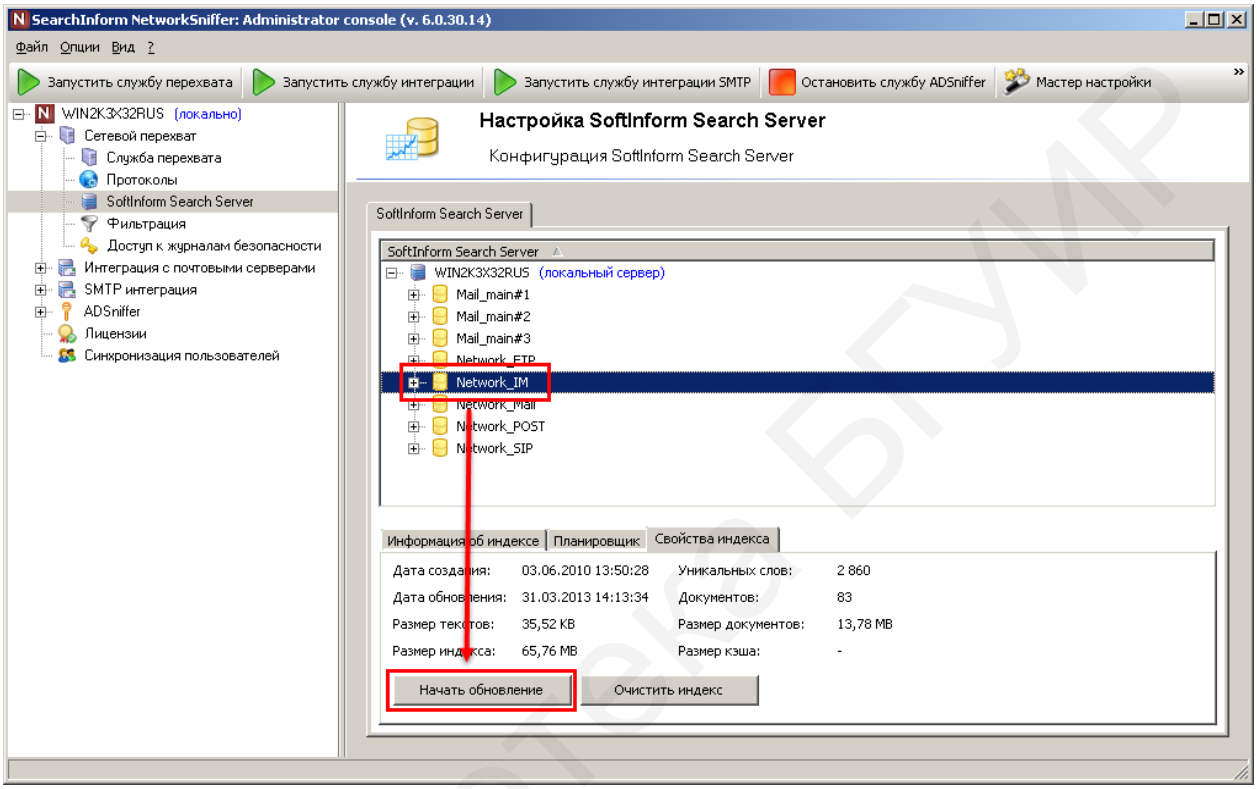


Рис. 2.14. Обновление индекса вручную

Очистка индекса позволяет удалить содержащиеся в индексе данные, не изменяя его свойств. Данную операцию рекомендуется использовать при восстановлении (переиндексации) поврежденного индекса. Для проведения очистки следует выделить индекс, перейти на вкладку «Свойства индекса» и воспользоваться кнопкой «Очистить индекс».

Для удаления индекса необходимо выделить индекс, открыть вкладку «Информация об индексе» и нажать кнопку «Удалить индекс». Одноименную операцию можно вызвать из контекстного меню.

Управление источниками данных. Источник данных – условный набор настроек базы или файлового хранилища, в которые помещена информация, обработанная сервером NetworkSniffer по одному протоколу; включает в себя настройки подключения к базе/хранилищу и имя протокола. Например, индексы IMSniffer, собранные при помощи NetworkSniffer, могут включать в себя источники данных шести типов, по одному на каждый протокол, для которого поддерживается запись в базы – ICQ, MSN, XMPP, MMP, HTTPIM, SIP, YAHOO.

Библиотека БГУИР

Текущий (активный) источник данных – модуль базы (хранилища), в который производится запись данных в момент перехвата. Запись данных, перехваченных по одному протоколу, можно производить только один раз.

Неактивный источник данных – модуль базы (хранилища), в котором содержатся перехваченные ранее (по протоколу) данные, но в который не записываются новые данные.

Привязанными к индексу источниками данных можно управлять. Если привязка протокола или продукта к БД (хранилищу) производится в отрыве от индексов, созданные ранее индексы перестают быть активными – в них больше не добавляются новые данные. Непривязанные к индексам активные источники данных можно добавить в любой зарегистрированный в консоли NetworkSniffer совместимый индекс.

Для добавления источника данных следует выделить индекс, к которому будет привязываться активный источник данных, затем нажать кнопку «Добавить источник данных» и выбрать активный источник данных (рис. 2.15).

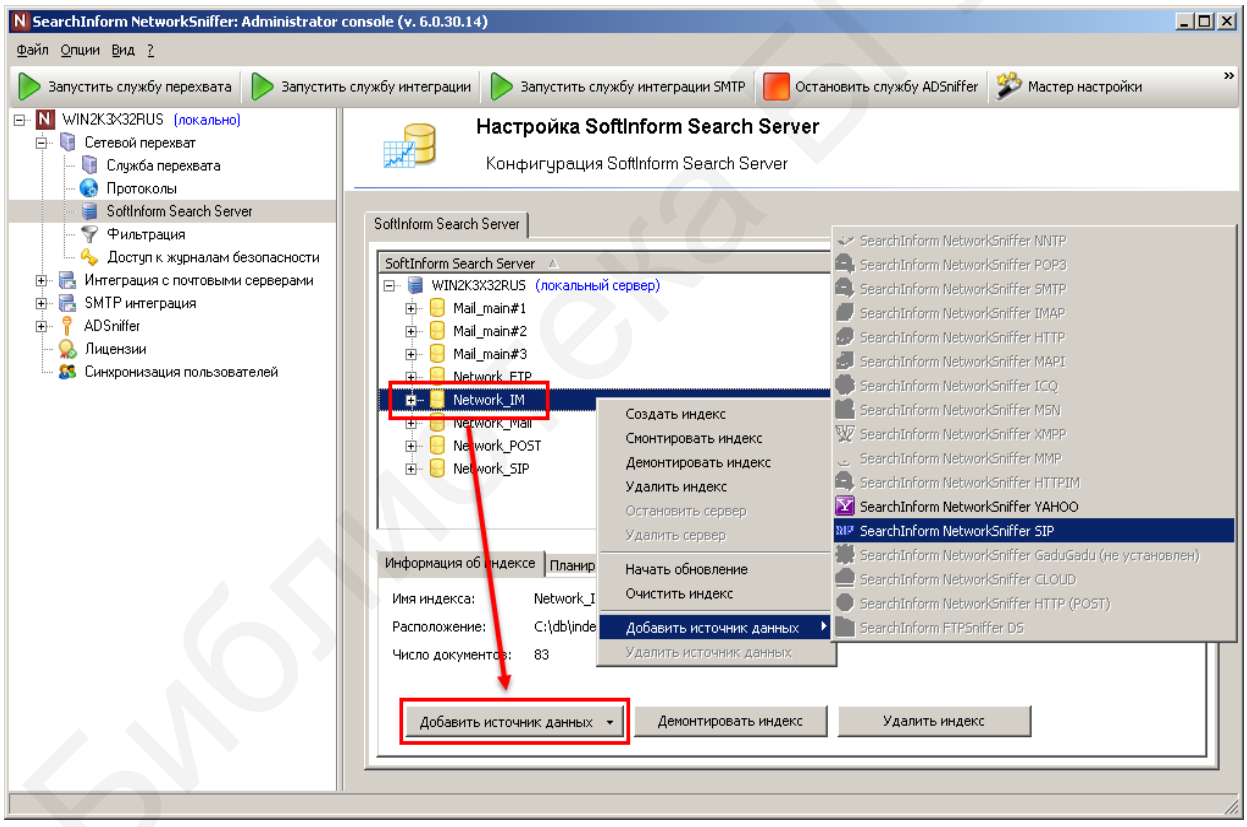


Рис. 2.15. Добавление источника данных

Записанная в источник данных информация станет доступной для поиска и анализа после обновления индекса.

Для удаления необходимо выделить источник данных и нажать кнопку «Удалить источник данных» (или выбрать одноименную команду из контекстного меню).

Библиотека БГУИР

Удаление привязки источника данных к индексу не влияет на запись перехваченной информации в базу (хранилище) – перехват данных и их запись в базу (хранилище) продолжаются, но перехваченная информация перестает быть доступной для поиска и анализа.

Подключение к существующему индексу. Для этого необходимо воспользоваться кнопкой «Смонтировать индекс» или одноименной командой из контекстного меню. Существует возможность подключить как локальный индекс, так и расположенный на удаленном сервере индексации.

Для подключения к локальному индексу на одноименной вкладке в открывшемся окне «Подключение существующего индекса» (рис. 2.16) следует нажать кнопку  для выбора файла индекса. После выбора индекса в нижней части окна будет отображена его статистика. Для завершения процедуры подключения необходимо нажать кнопку «Добавить».

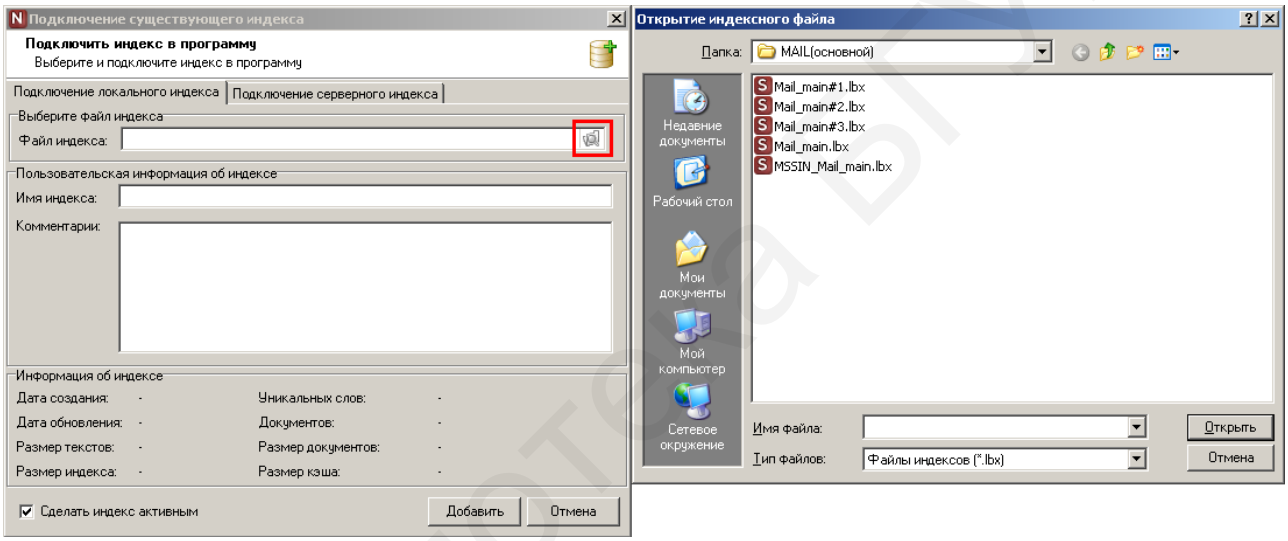


Рис. 2.16. Подключение к локальному индексу

Для подключения к удаленному индексу в окне «Подключение существующего индекса» следует перейти на вкладку «Подключение серверного индекса», после чего воспользоваться выпадающим списком «Сервер» для обнаружения требуемого сервера (рис. 2.17).

После выбора индекса в нижней части окна будет отображена его статистика. Для завершения процедуры подключения необходимо нажать кнопку «Добавить».

Библиотека БГУИР

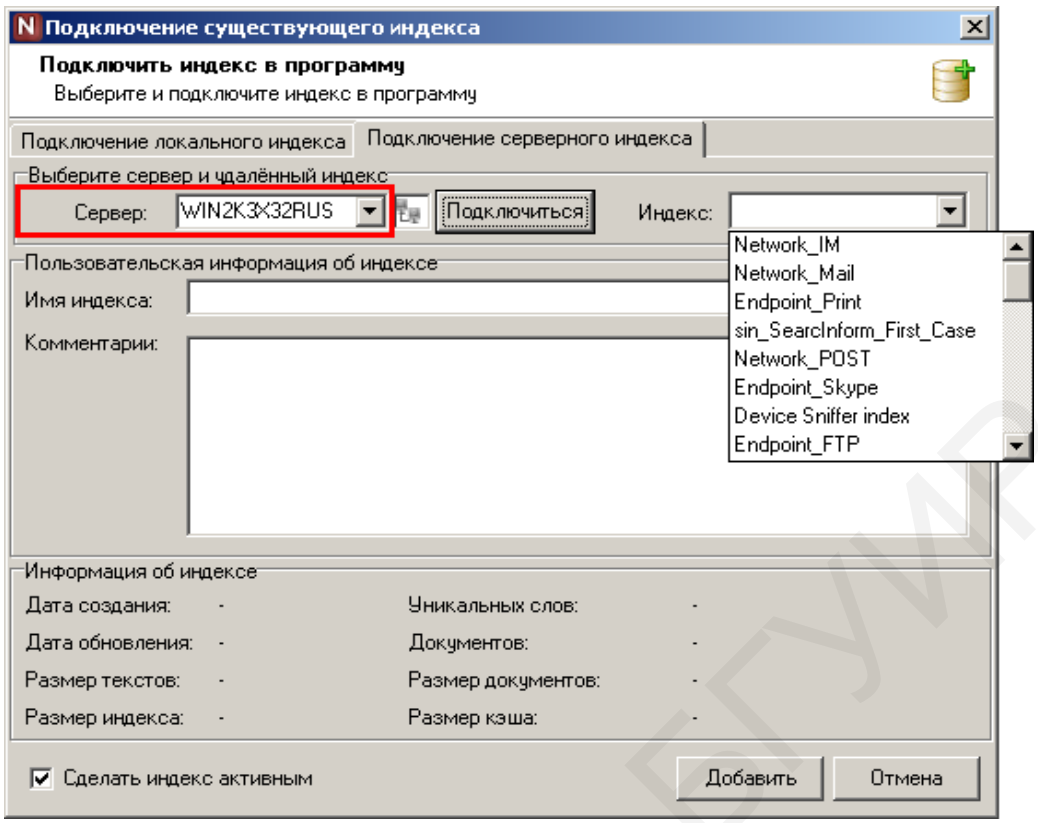


Рис. 2.17. Подключение к удаленному индексу

Фильтрация трафика. Сервер NetworkSniffer работает на уровне сетевых шлюзов и перехватывает весь интернет-трафик. Однако может возникнуть необходимость обработать не весь трафик, а только его часть. Для этого предусмотрена функция фильтрации, которая позволяет обрабатывать только те сообщения, которые были отправлены или получены целевыми пользователями.

Обычно фильтрация производится по атрибутам сетевых пакетов – доменному имени пользователя, имени компьютера, IP- и MAC-адресам.

Сетевые пакеты, перенаправленные из узла сети, расположенного между прокси-сервером и интернет-шлюзом, не имеют атрибутов, указывающих на конкретных пользователей. Поэтому для фильтрации сообщений, перехваченных в такой точке, предусмотрена функция фильтрации по почтовым признакам и прокси-серверам.

HTTP-фильтрация позволит отсечь лишний мусор, например, можно исключить из перехвата запросы к внутренним веб-системам или указать почтовые хосты, с которых не требуется перехват трафика.

Порядок фильтрации:

– вне зависимости от параметров фильтрации, сервер NetworkSniffer анализирует весь сетевой трафик;

– сервер NetworkSniffer сверяет атрибуты каждого полученного пакета данных по имеющимся фильтрам;

– если фильтры не были установлены, фильтрация не происходит, и все пакеты данных без исключения передаются на сервер баз данных или в хранилище;

Библиотека БГУИР

– если фильтры были настроены, перехват будет осуществляться согласно заданным условиям.

Настройка фильтрации по атрибутам производится на вкладке «Фильтрация».

Одновременно можно использовать или запрещающие, или разрешающие фильтры:

– при запрещающей фильтрации будут обработаны все сетевые пакеты, за исключением совпадений с настроенными условиями; должна быть включена опция «Исключить из перехвата трафика»;

– при разрешающей фильтрации будут обработаны только сетевые пакеты, совпадающие с настроенными условиями; должна быть включена опция «Включить в перехват трафика».

Если фильтрация включена (разрешающая или запрещающая), но условия не настроены (список фильтров пуст), обработка сетевых пакетов осуществляется без ограничений.

Чтобы сетевой пакет попал под действие правила («Запретить перехват» или «Разрешить перехват»), достаточно совпадения по одному атрибуту. Глобальные фильтры применяются ко всем протоколам. Настройка производится на вкладке «Глобальные настройки» (рис. 2.18).

Фильтры протоколов применяются только к отдельным протоколам. Операция производится на вкладке «Настройки протоколов». Для настройки такого фильтра необходимо выделить протокол и воспользоваться кнопкой «Добавить» (рис. 2.19).

Условие глобальной фильтрации можно отменить для отдельных протоколов – для этого нужно снять соответствующий флажок.

Для настройки фильтров можно использовать четыре типа условий:

– пользователи домена;

– имена компьютеров;

– IP-адреса пользователей;

– MAC-адреса пользователей.

Для управления фильтрами используются кнопки «Добавить», «Удалить» и «Изменить».

При настройке фильтра по пользователям домена можно вручную ввести одного или нескольких пользователей. Ввод нескольких пользователей производится через запятую. Допускается использование метасимвола «*», заменяющего от нуля и более символов, в имени пользователя. Также можно воспользоваться кнопкой  и получить список пользователей из DataCenter, Active Directory или NetBIOS.

При настройке фильтра по имени компьютера следует указать тип фильтра и имя нужного компьютера. При этом, как и в предыдущем случае, допускается использование метасимвола «*» в имени компьютера. Также можно воспользоваться кнопкой  и выбрать компьютеры с помощью обозревателя.

Библиотека БГУИР

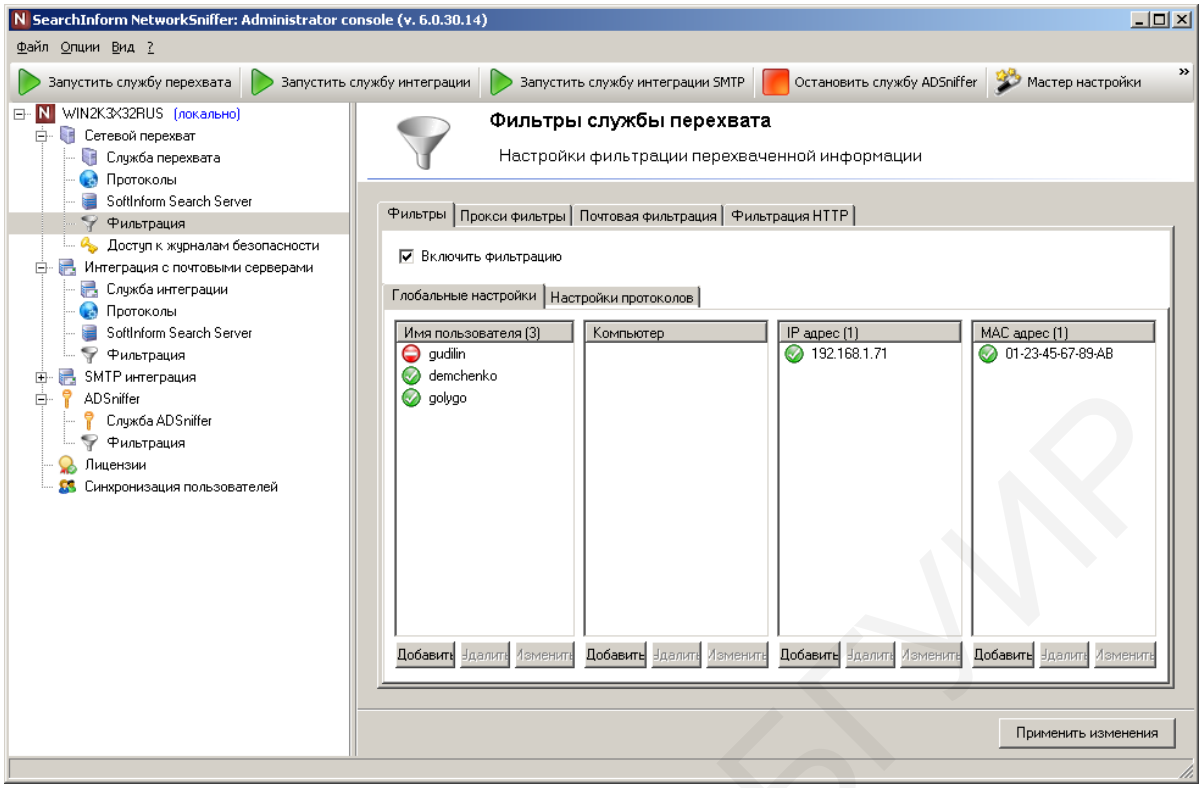


Рис. 2.18. Глобальные настройки

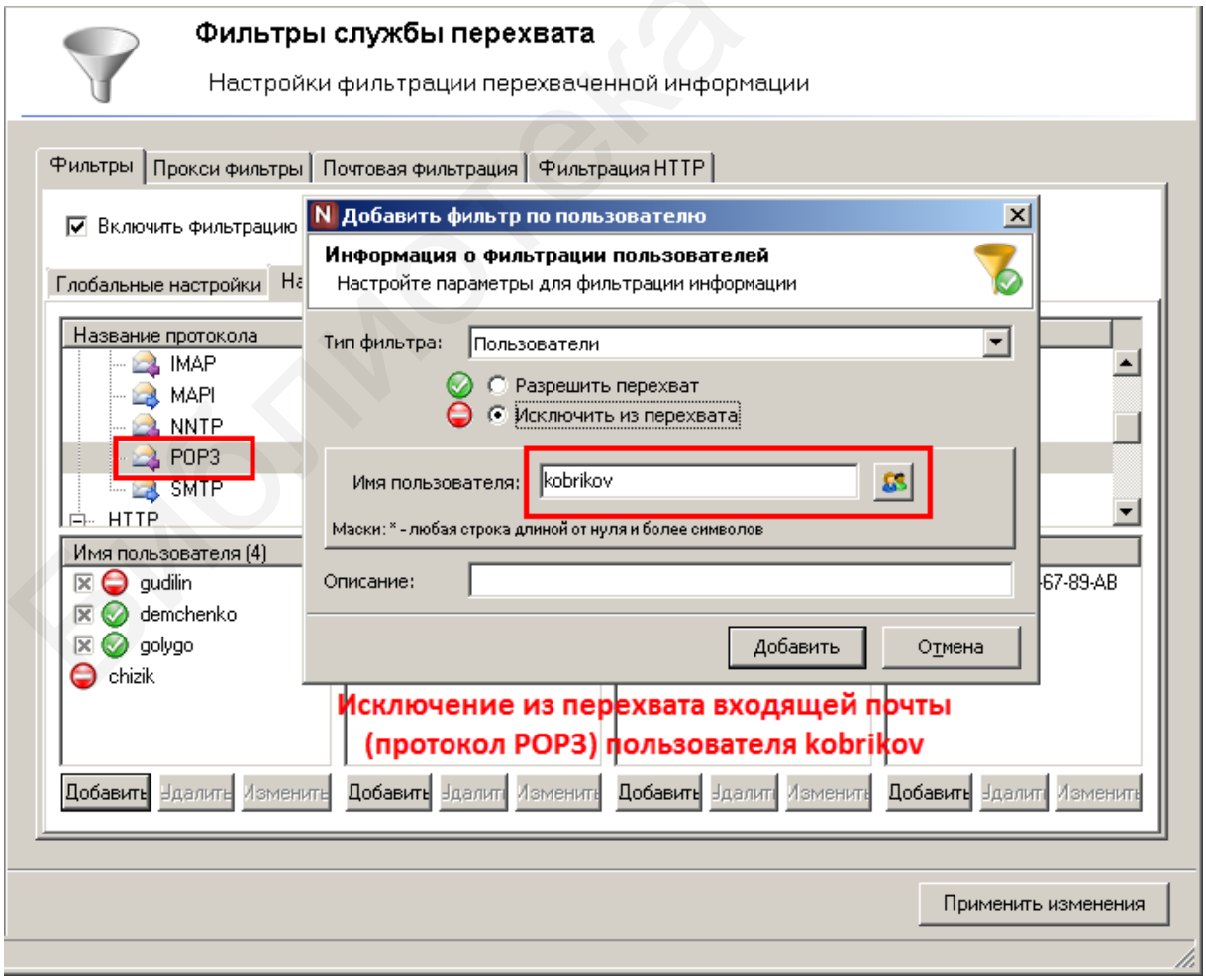


Рис. 2.19. Фильтры протоколов

Для осуществления фильтрации по IP-адресу можно применить один из трех типов фильтров: по отдельным IP-адресам, по сетевой маске и по диапазону IP-адресов.

Для добавления фильтра по MAC-адресу необходимо ввести его значение в соответствующее поле.

Примеры настройки фильтров по атрибутам сетевых пакетов представлены на рис. 2.20.

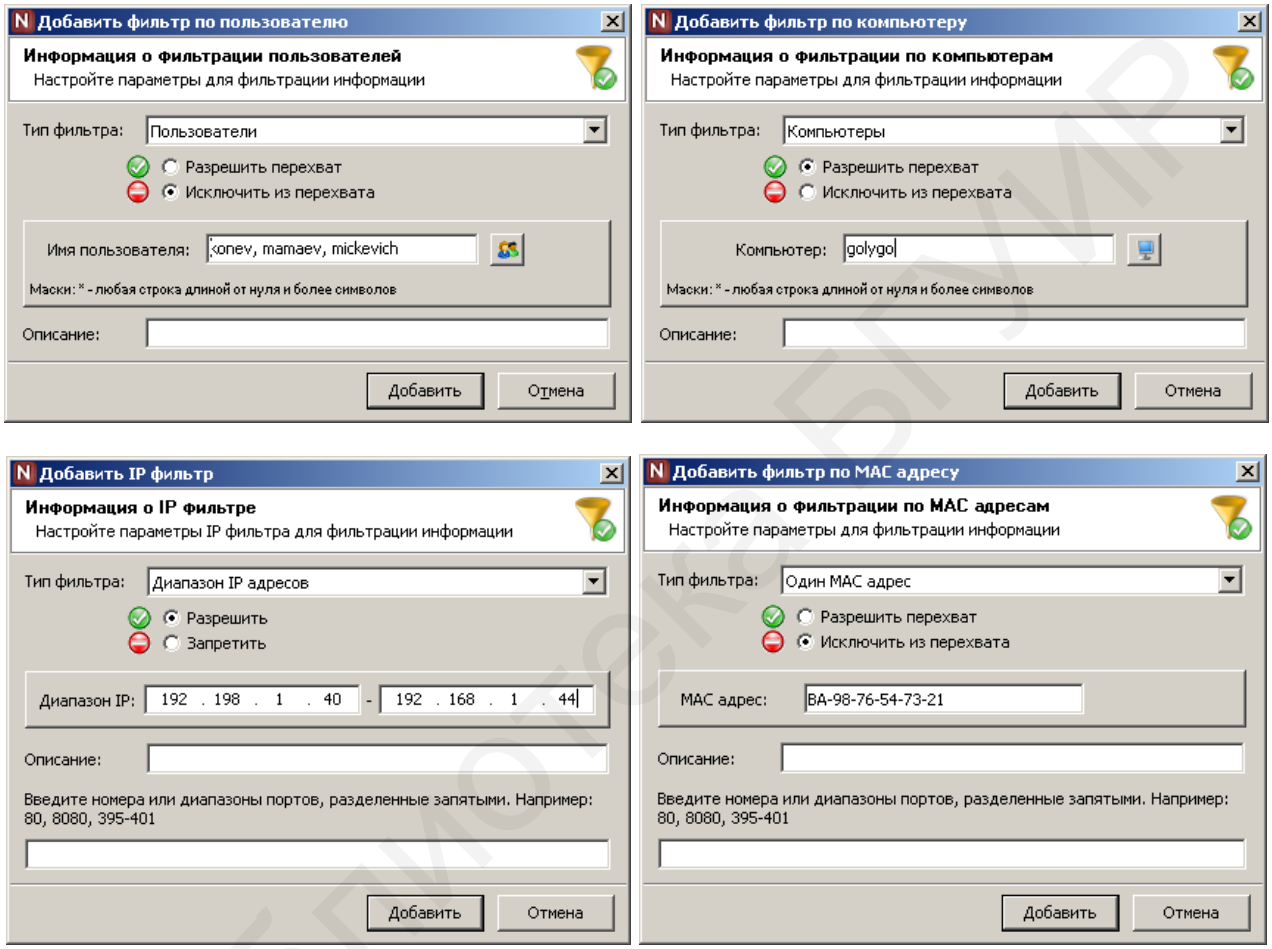


Рис. 2.20. Настройка фильтров

При установке NetworkSniffer после прокси-сервера или почтового сервера фильтрация по доменным именам и IP/MAC-адресам не работает, т. к. перехваченные в этой точке сетевые пакеты не имеют этих атрибутов (видны только IP/MAC-адреса почтового или прокси-сервера).

Другая проблема, связанная с установкой NetworkSniffer после прокси-сервера, состоит в том, что протокол SMTP может использоваться не только для отправки, но и для получения почты (внешние серверы могут доставлять данные на корпоративный адрес по SMTP-протоколу). Поэтому предусмотрена возможность указать IP-адреса внутренних почтовых и прокси-серверов, благодаря чему NetworkSniffer сможет определить направление почты и отфильтро-

Библиотека БГУИР

вать те сообщения, которые не нужно обрабатывать, например, сообщения, отправленные руководством, массовые рассылки и др.

Для настройки фильтрации по прокси-серверам следует перейти на вкладку «Прокси фильтры», установить флажок в строке «Прокси фильтры» и воспользоваться кнопкой «Добавить». В качестве фильтра добавляется IP-адрес внутреннего прокси-сервера.

Почтовая фильтрация ориентирована только на действия, связанные с перехватом сообщений, передаваемых при помощи протоколов электронной почты. Для настройки фильтров предназначена вкладка «Почтовая фильтрация» (рис. 2.21). Для активации указанной фильтрации следует установить флажок в строке «Включить фильтрацию», а для непосредственной настройки фильтра – воспользоваться кнопкой «Добавить».

В открывшейся справа области необходимо выбрать протокол, к которому будет применен фильтр, и указать параметры фильтра, предварительно установив соответствующие флажки. При этом рекомендуется, чтобы обрабатываемые доменные имена и адреса получателей/отправителей сообщений начинались и заканчивались маской с символом «*», подразумевающим любое количество и сочетание символов.

Примеры масок:

– *ivan.ivanov@company.ru*

– *@company.ru*

– *ivan.*@company*

– *ivan.ivanov*

– *ivan*.

В случае когда в фильтре содержатся имена и отправителя, и получателя, с помощью переключателей «И/ИЛИ» необходимо указать, должны ли совпадать оба имени при проверке по данному фильтру либо достаточно одного любого совпадения.

Для выбора доменных имен отправителей и/или получателей из списка используется кнопка «Добавить».

В диалоговом окне «Выбор пользователя» следует отметить нужного пользователя и подтвердить выбор кнопкой «Применить». Если список пользователей достигает больших размеров, можно воспользоваться строкой поиска.

Библиотека БГУИР

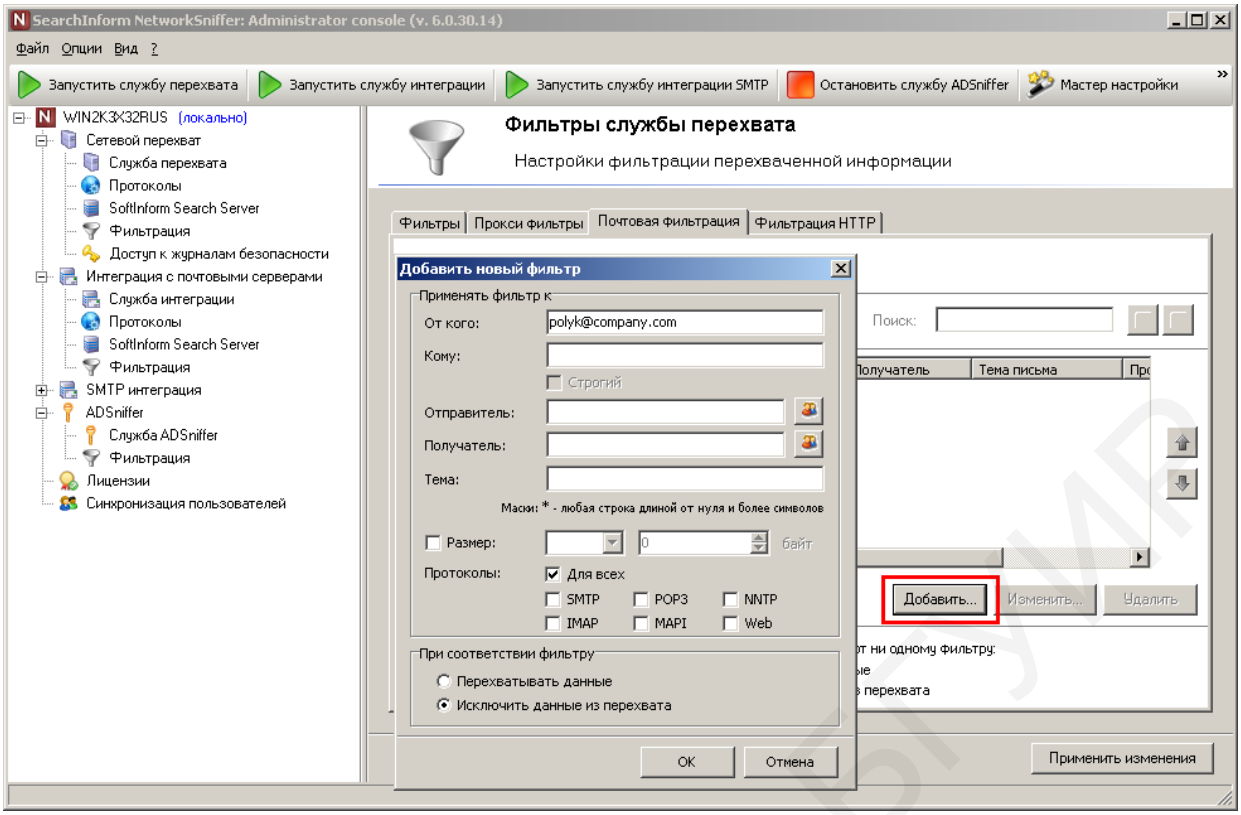


Рис. 2.21. Почтовая фильтрация

Фильтрация может быть как разрешающей (производится запись в базу), так и запрещающей (запись в базу не производится). В группе «При соответствии фильтру» можно выбрать соответствующую опцию «Сохранить письмо» или «Исключить письмо».

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает. Управление порядком фильтров производится с помощью кнопок с изображением стрелок (вверх/вниз).

При использовании параметра «Строгий» фильтр сработает, если условиям фильтра удовлетворяет хотя бы один адресат. Он сохранит/не сохранит документ в базу и запретит обработку всех следующих за ним фильтров. При снятом флажке (нестрогий фильтр) запоминается сработавшее состояние и последовательная работа остальных фильтров продолжается. Нестрогий фильтр сработает только тогда, когда под условие одного или нескольких фильтров попадут все адресаты.

Также есть возможность установить действие по умолчанию в том случае, если письмо не будет соответствовать ни одному из фильтров: либо «Перехватывать письмо», либо «Исключить письмо из перехвата».

Для поиска по списку заданных фильтров необходимо указать значение атрибута, по которому будет производиться поиск, в поле «Фильтр», после чего выбрать в выпадающем списке сам атрибут. При этом в области фильтров отобразятся только фильтры, отвечающие введенному значению (если таковые имеются).

Библиотека БГУИР

Для сохранения и загрузки списка фильтров предусмотрены кнопки «Экспорт» и «Импорт». Поддерживаются форматы .lst, .txt и .csv.

Фильтрация HTTP. Фильтры работают для GET/POST-запросов, передаваемых по протоколу HTTP. Для настройки фильтрации следует перейти на вкладку «Фильтрация HTTP», установить флажок в строке «Включить фильтрацию», после чего нажать кнопку «Добавить» (рис. 2.22). В открывшейся справа области необходимо указать значения атрибутов документа, к которым будет применен фильтр, предварительно установив напротив него флажок:

– «Хост» – адрес ресурса в сети;
– «Содержимое» – данные GET/POST-запроса;
– «Отправитель» – полное доменное имя отправителя запроса;
– «Размер» – размер запроса.

В имени хоста и отправителя допускается использование метасимвола «*».

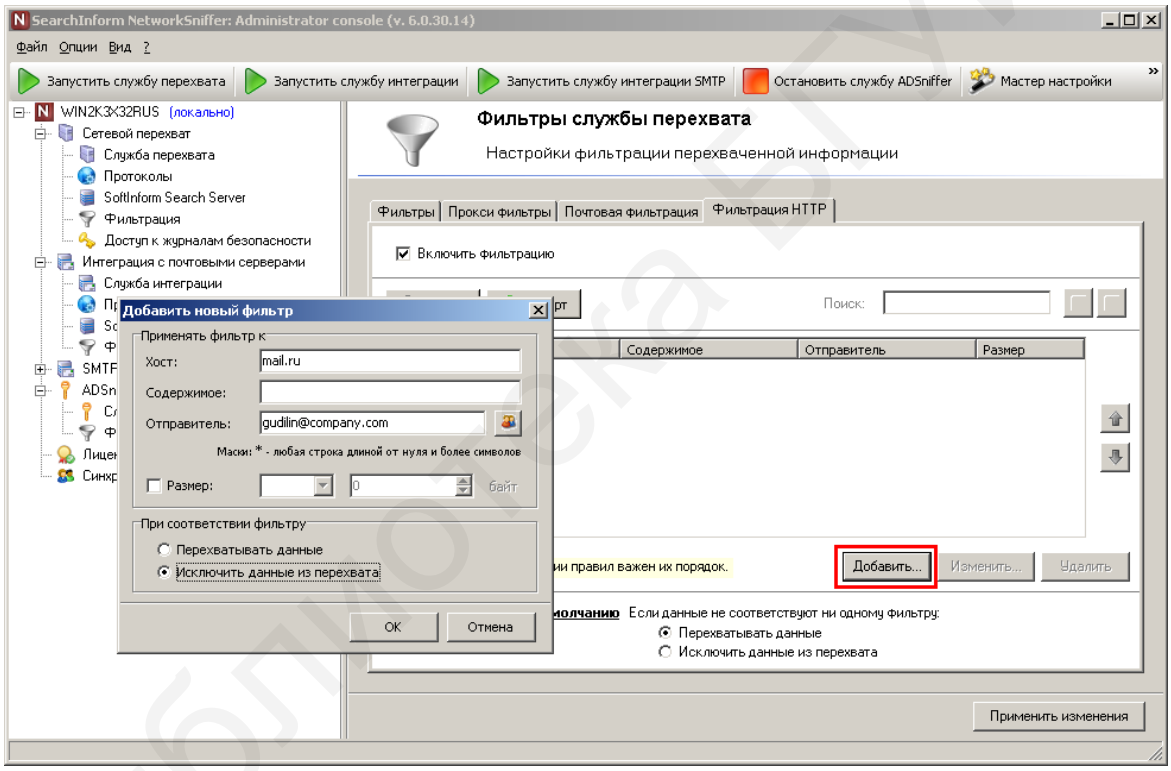


Рис. 2.22. Фильтрация HTTP

Фильтрация может быть как разрешающей (производится запись в базу), так и запрещающей (запись в базу не производится). В группе «При соответствии фильтру» можно выбрать соответствующую опцию «Сохранить документ» или «Исключить письмо».

Аналогично почтовой фильтрации есть возможность установить действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать документ», либо «Исключить документ из перехвата».

Доступ к журналам безопасности. В домене может быть несколько контроллеров домена, проводящих аутентификацию пользователей и обеспе-

Библиотека БГУИР

чивающих политику безопасности домена. Каждый контроллер домена обслуживает только свой домен.

Подключение к контроллерам домена может производиться от разных учетных записей. Для этого необходимо выбрать узел «Доступ к журналам безопасности» группы узлов «Сетевой перехват» и установить флажок напротив параметра «Использовать следующую информацию для доступа к журналам безопасности». Далее необходимо щелкнуть кнопку «Добавить», указать контроллер домена, полное имя пользователя в формате domain\user или user@domain.local и пароль для доступа к журналам безопасности (рис. 2.23).

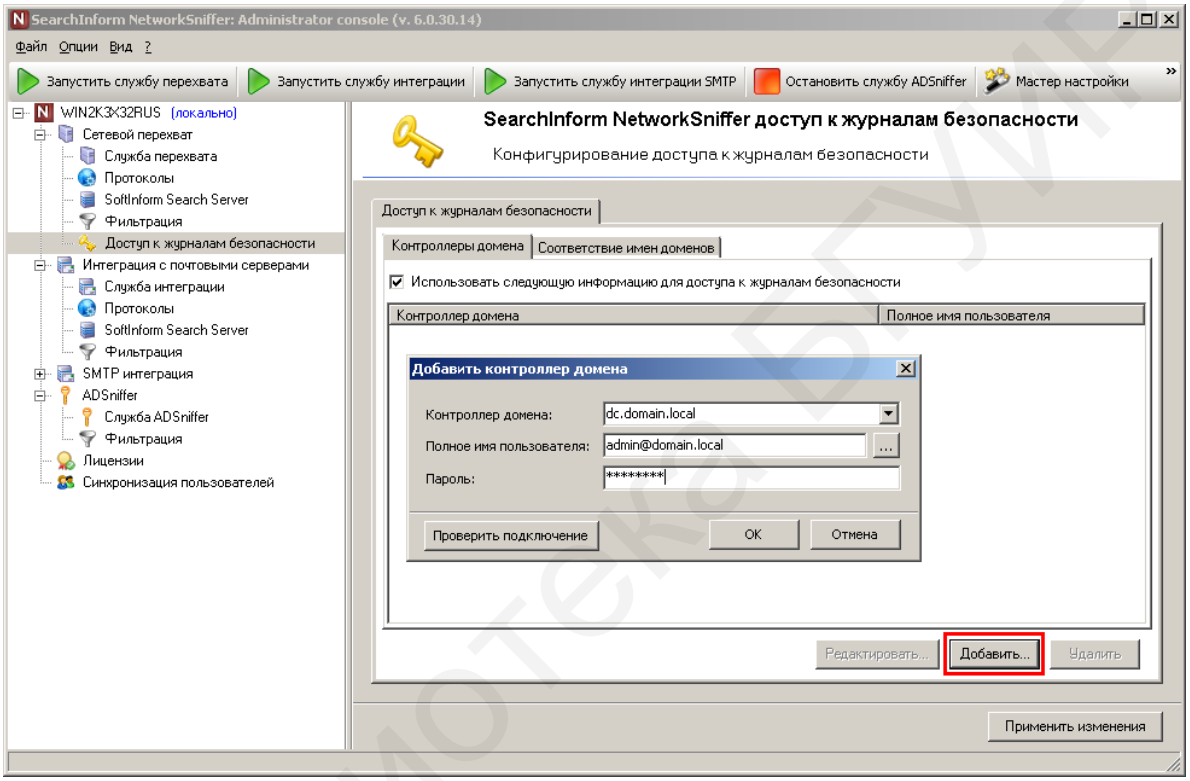


Рис. 2.23. Доступ к журналам безопасности

Проверка корректности введенных данных для подключения производится нажатием кнопки «Проверить подключение».

2.2. Платформа SearchInform NetworkSniffer: особенности реализации перехвата почтовых сообщений путем интеграции с почтовыми серверами и/или SMTP-интеграции

Сервер NetworkSniffer включает в себя службу интеграции с почтовыми серверами, предназначенную для сбора почтовых сообщений напрямую с почтового сервера, и службу SMTP-интеграции, предназначенную для перехвата трафика журналирования почтовых серверов.

Интеграцию с почтовыми серверами/SMTP-интеграцию можно комбинировать с перехватом сетевого трафика.

Библиотека БГУИР

Функции службы:

– сбор сообщений с почтовых серверов;

– обработка полученных данных и их запись в базу данных, которая может быть обработана поисковым движком.

Настройка производится в соответствующих узлах «Интеграция с почтовыми серверами» / «SMTP интеграция».

Далее будет рассмотрена настройка на примере службы интеграции с почтовыми серверами. Настройка службы SMTP-интеграции производится аналогично.

Служба интеграции. Настройка параметров работы службы интеграции осуществляется на вкладке «Параметры сервиса» узла «Служба интеграции» (рис. 2.24).

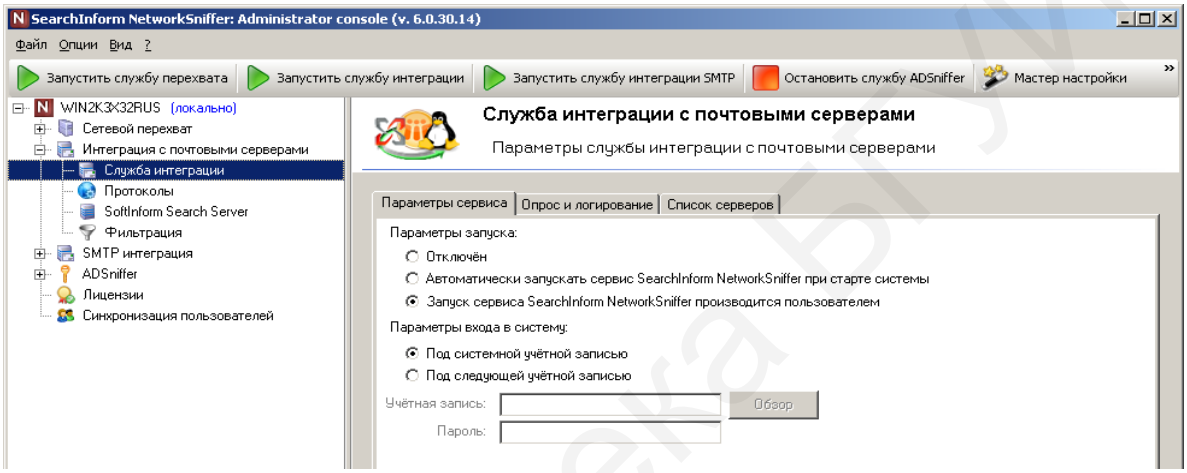


Рис. 2.24. Настройка службы интеграции

Обеспечены следующие возможности настройки службы:

– выбор типа запуска – «Автоматически», «Вручную», «Отключена»;

– выбор учетной записи, под которой будет работать служба.

Требования к учетной записи службы интеграции:

– возможность входа в качестве службы на сервере NetworkSniffer;

– право получения списка пользователей из каталога Active Directory.

В большинстве случаев для запуска службы достаточно системной учетной записи.

Настройка уровня логирования и интервала сбора сообщений с почтовых серверов производится на вкладке «Опрос и логирование». Для нормальной работы рассматриваемой службы на указанной вкладке следует установить необходимый интервал синхронизации с почтовым сервером. При этом под интервалом синхронизации понимается частота, с которой сервис интеграции получает сообщения с почтового сервера. Интервал синхронизации задается в минутах. Минимальное рекомендуемое значение – 10 минут.

Протоколирование службы интеграции может потребоваться в целях проведения диагностики функционирования системы. Настройка уровня логирования производится в группе «Уровень логирования». Доступны следующие значения:

Библиотека БГУИР

– «Обычный» – фиксируются серьезные ошибки службы синхронизации и консоли управления сервером, повлекшие прерывание или аварийное завершение работы, запуск внутренних функций программы;

– «Детальный» – дополнительно фиксируется запуск внутренних функций программы в подробном виде; данный режим рекомендуется включать только по запросу сотрудников службы технической поддержки в случае критических проблем с сервером.

Для сохранения на жесткий диск почтовых сообщений, не прошедших лицензирование, отметьте соответствующий параметр.

При отметке флажком параметра «Сохранять e-mail письма в файлы» все почтовые сообщения будут экспортироваться во внешние файлы.

Для настройки подключения к почтовому серверу используется вкладка «Список серверов».

Сбор сообщений с почтовых серверов производится по протоколу POP3. Если для сбора почтовых сообщений используется несколько учетных записей электронной почты, для каждой из них нужно настроить отдельное подключение. Для добавления подключения необходимо нажать кнопку «Добавить сервер» и ввести имя почтового сервера (рис. 2.25).

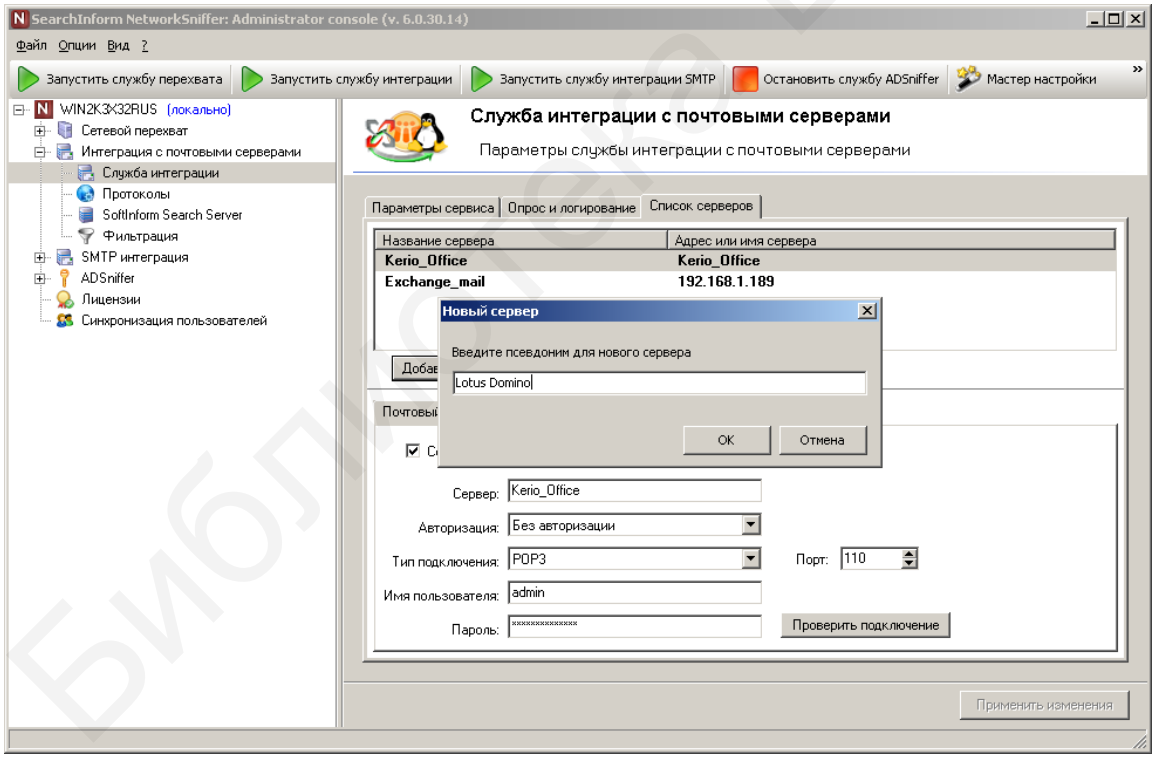


Рис. 2.25. Настройка подключения к почтовому серверу

Убедившись, что почтовый сервер сконфигурирован корректно, следует ввести настройки, совпадающие с параметрами, которые используются при конфигурации почтового сервера для получения перенаправленных сообщений, а именно:

– имя или IP-адрес почтового сервера;

– тип авторизации: без авторизации, обычная, MD5SRAM-запрос;

– тип подключения: обычное, безопасное на специальный порт (TLS), безопасное на обычный порт (STARTTLS);

– имя пользователя;

– пароль.

Дополнительно к этому необходимо выбрать действие по отношению к сообщениям на почтовом сервере (вкладка «Управление почтой»). Возможные варианты (рис. 2.26):

– не удалять;

– удалять после прочтения;

– удалить после (указать интервал в днях).

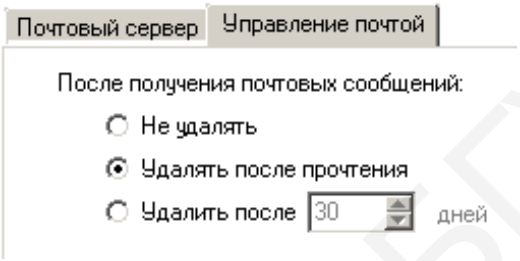


Рис. 2.26. Выбор действия после получения почтовых сообщений

Управление протоколами. Модуль интеграции с почтовыми серверами включает два условных протокола:

– Mail server (out) – исходящие сообщения;

– Mail server (in) – входящие сообщения.

Для обработки всех собранных с почтовых серверов сообщений необходимо для каждого из протоколов настроить подключение к базе данных. При этом возможна привязка как обоих протоколов к одной базе данных, так и каждого к отдельной.

Для привязки протокола к базе необходимо перейти на вкладку «Протоколы» узла «Служба интеграции» (рис. 2.27), выделить протокол и, нажав кнопку «Настроить хранилище данных», осуществить настройку подключения к серверу Microsoft SQL, в ходе которой произвести следующие действия:

– ввести имя или IP-адрес сервера Microsoft SQL;

– выбрать метод аутентификации – аутентификация Windows или внутренняя аутентификация сервера Microsoft SQL (рекомендуемый метод – внутренняя аутентификация Microsoft SQL);

– в случае внутренней аутентификации Microsoft SQL ввести имя и пароль пользователя с правами на запись информации.

Для создания базы данных следует нажать кнопку «Создать» и ввести имя новой базы. При подключении к уже созданной базе данных достаточно выбрать ее в выпадающем списке.

Библиотека БГУИР

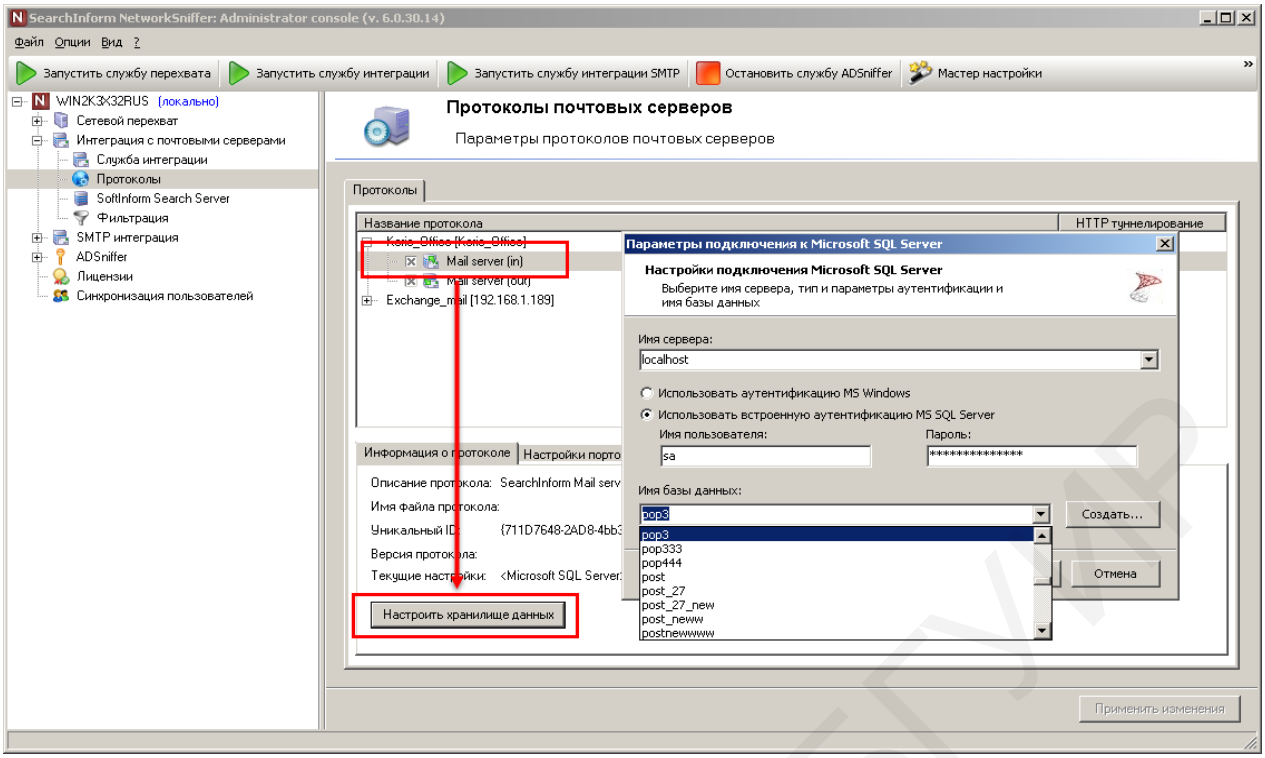


Рис. 2.27. Привязка протокола к базе данных

Для включения модулей обработки протоколов необходимо установить соответствующие флажки . В результате настройки соответствующие протоколы должны быть включены, причем для каждого из протоколов должна отображаться привязанная база данных.

Работа с индексами собранных сообщений. Поиск по почтовым сообщениям и их анализ производится через индексы поисковой подсистемы. Для осуществления операций с индексами локально или в сети должен быть установлен SoftInform Search Server. С помощью консоли NetworkSniffer можно создавать только индексы протоколов, запись которых в базу данных производится самим сервером.

Настройка индексов данных, собранных с почтовых серверов, производится на вкладке «SoftInform Search Server» группы узлов «Интеграция с почтовыми серверами» (рис. 2.28), а также в окне «Мастер быстрой настройки».

Запуск/остановка сервера SoftInform Search производится путем нажатия кнопки «Запустить сервер/Остановить сервер» (в зависимости от его текущего состояния). Кнопка «Удалить сервер» позволяет удалить выбранный сервер индексации из списка в консоли NetworkSniffer.

Стандартными операциями с индексами, которые могут быть осуществлены в консоли администратора, являются:

– создание индекса;
– обновление индекса по расписанию или вручную;
– очистка и удаление индекса;
– добавление и удаление источников данных;
– подключение существующего индекса.

Библиотека БГУИР

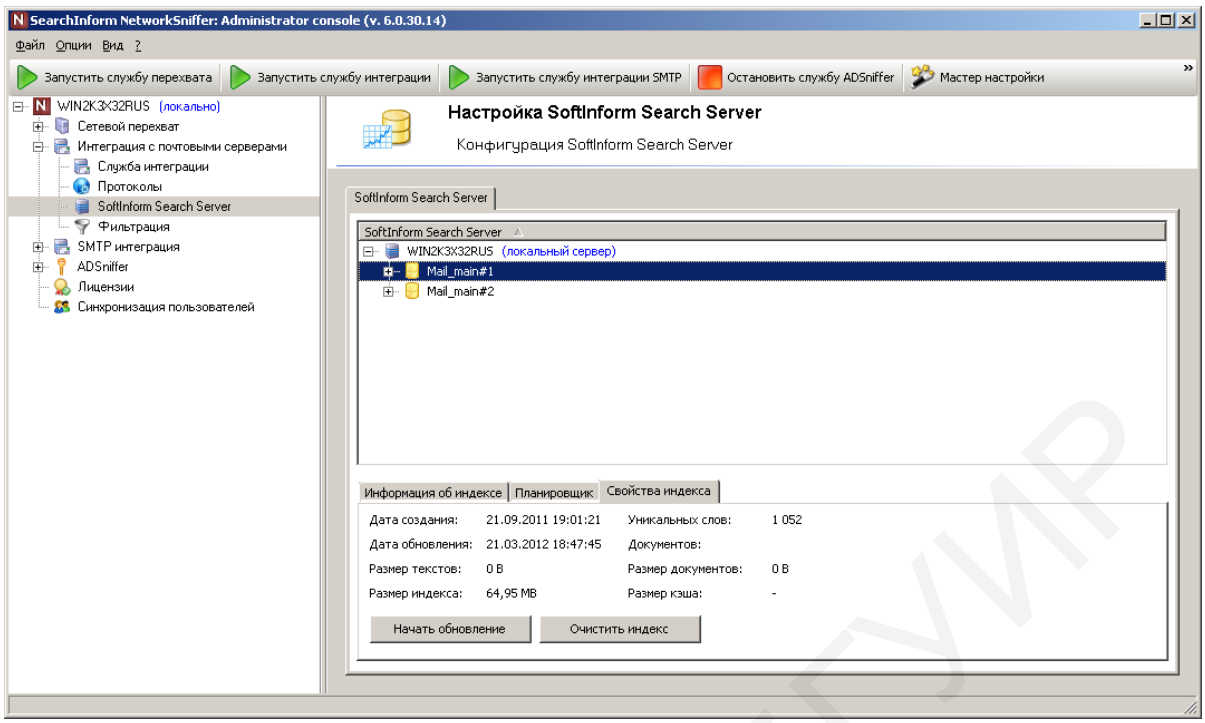


Рис. 2.28. Работа с индексами собранных сообщений

Создание индексов производится либо из консоли администрирования NetworkSniffer, либо из серверной консоли SoftInform Search.

Тем не менее для создания новых индексов рекомендуется использовать консоль сервера NetworkSniffer, т. к. в этом случае происходит привязка баз данных к активному протоколу (сервер NetworkSniffer сохраняет новые перехваченные сообщения и файлы в указанную базу данных). Создавать индексы из консоли сервера SoftInform Search следует только для баз, которые больше не будут использоваться для записи новых документов.

Для создания индекса предназначена кнопка «Создать индекс». При помощи мастера следует выполнить следующие шаги:

– выбрать сервер SoftInform Search или ввести его имя/IP-адрес;

– настроить подключение к базе данных (создать новую или подключиться к уже существующей); в отличие от функции «Мастер создания индекса» при сетевом перехвате данных отсутствует возможность выбора СУБД – собранные сообщения можно записать только в базы данных под управлением Microsoft SQL Server;

– выбрать протоколы данных, включенных в индекс; при этом NetworkSniffer будет складывать сообщения, перехваченные по указанным протоколам, в подключенную БД;

– ввести имя индекса и выбрать директорию, по которой индекс будет храниться.

Новый индекс будет отображен в консоли NetworkSniffer. Для созданного индекса рекомендуется настроить расписание обновления.

Запуск обновления индекса, очистка и удаление индекса осуществляются аналогично тому, как это было рассмотрено для сетевого перехвата данных. То же можно сказать и об управлении источниками данных, а также подключении ло-

Библиотека БГУИР

кальных или удаленных индексов. При этом следует помнить, что индекс сообщений, собранных с почтовых серверов, включает в себя два источника данных – Mail Servers (in) и Mail Servers (out), для которых поддерживается запись в базу данных. Если для входящих и исходящих сообщений созданы отдельные базы данных (и индексы), каждая из них будет содержать только свой источник данных.

Синхронизация пользователей. В узле «Синхронизация пользователей» отображаются настройки, позволяющие установить параметры фильтрации сообщений и идентификации пользователей.

Фильтрация сообщений может потребоваться для отмены мониторинга заданных пользователей либо приведения параметров в соответствие с требованиями лицензии.

Для правильного использования фильтрации необходимо помнить, что полученное с почтового сервера сообщение имеет два пользовательских атрибута – адрес отправителя и адрес получателя (может быть и несколько получателей). Для выполнения условия достаточно совпадения по одному адресу.

Алгоритм фильтрации сообщений следующий.

1. Собранные с сервера почтовые сообщения не имеют формальных признаков, позволяющих определить конкретных доменных пользователей. Для идентификации доменных пользователей используются привязки почтовых адресов к доменным именам. Если найдено совпадение, сообщение проверяется по дополнительным фильтрам (п. 3). Если совпадений не найдено, осуществляется переход к п. 2.

2. Полученное почтовое сообщение проверяется по настроенным маскам. Если найдено совпадение, сообщение записывается в базу. Если совпадений не найдено, сообщение не будет перехвачено.

3. Сообщения, предварительно отсортированные по привязкам почтовых адресов и по настроенным маскам, последовательно проверяются по дополнительным фильтрам. При срабатывании по первому выполненному условию проверка прекращается и сообщение либо записывается в базу (разрешающее условие) либо отфильтровывается (запрещающее условие). Если совпадений не найдено, проверяется действие по умолчанию.

Настройка привязки доменных пользователей к почтовым адресам и/или масок адресов при интеграции с почтовыми серверами либо SMTP-интеграции является обязательной. В случае их отсутствия ни одно из писем не будет перехвачено (независимо от условий дополнительных фильтров).

При интеграции с почтовыми серверами письма не содержат явной информации о направлении переписки (только адреса отправителя и получателя). В ходе проверки письма согласно пп. 1 и 2 определяется, адрес какого из полей сообщения («От кого» или «Кому») соответствует доменному имени пользователя (или прошел по маске). Если удалось идентифицировать отправителя (поле «От кого»), письмо помечается как исходящее и записывается в соответствующую базу данных (при условии, что для протоколов POP3 и SMTP созданы разные базы). Если же определен получатель (поле «Кому»), письмо считается входящим.

Библиотека БГУИР

Привязки почтовых адресов к доменным адресам можно осуществлять следующим образом:

– получать из Active Directory;

– вводить вручную.

Привязка доменных имен к почтовым адресам производится на вкладке «Синхронизация пользователей» (рис. 2.29). Доменное имя присваивается только тем сообщениям, которые имеют настроенный адрес электронной почты в поле «Отправитель» или «Получатель» (первое найденное значение, если есть несколько получателей).

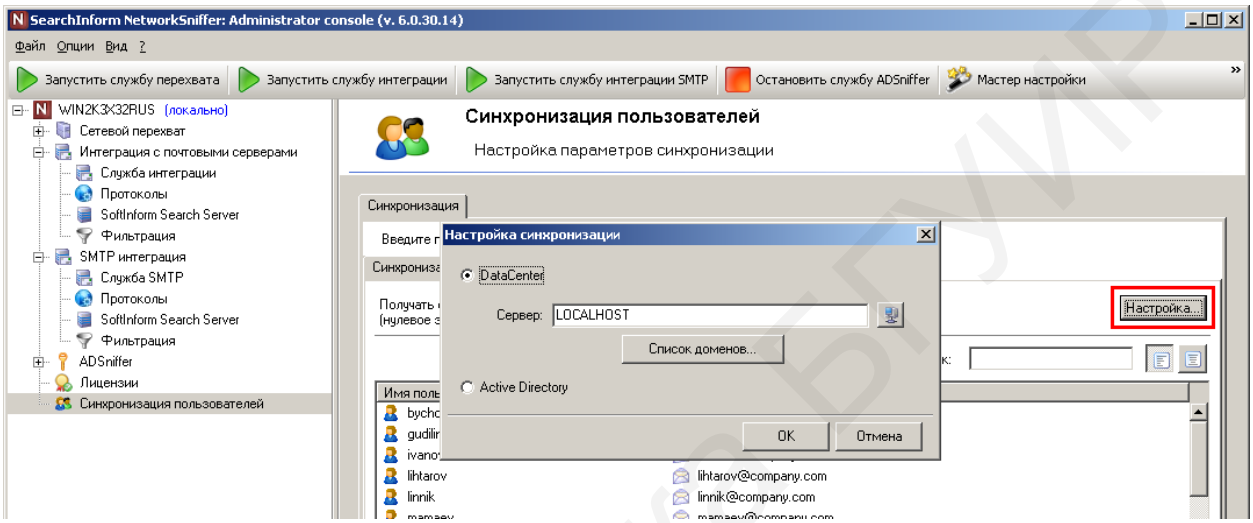


Рис. 2.29. Вызов окна настроек синхронизации

Получение доменных имен из Active Directory. Благодаря данной функции служба интеграции сможет получить из DataCenter либо каталога Active Directory все имена доменных пользователей, к которым привязаны почтовые адреса (только для тех пользователей, к которым привязаны почтовые адреса). Служба интеграции с почтовыми серверами либо служба SMTP-интеграции должна иметь право чтения каталога Active Directory.

С помощью кнопки «Настройка» задаются параметры синхронизации. При синхронизации с DataCenter необходимо задать имя сервера и выбрать необходимые домены. При синхронизации с Active Directory вычитывается только текущий домен.

Для получения доменных имен из каталога Active Directory следует ввести интервал синхронизации в поле «Получать список пользователей каждые … дней», применить изменения, нажав кнопку «Применить изменения», и перезапустить службу интеграции с почтовыми серверами.

Получение доменных имен можно осуществить и вручную, нажав кнопку «Получить из Active Directory» (рис. 2.30). Пользователей, не имеющих e-mail адресов, можно удалить из списка при помощи кнопки «Удалить пользователей без почты».

Библиотека БГУИР

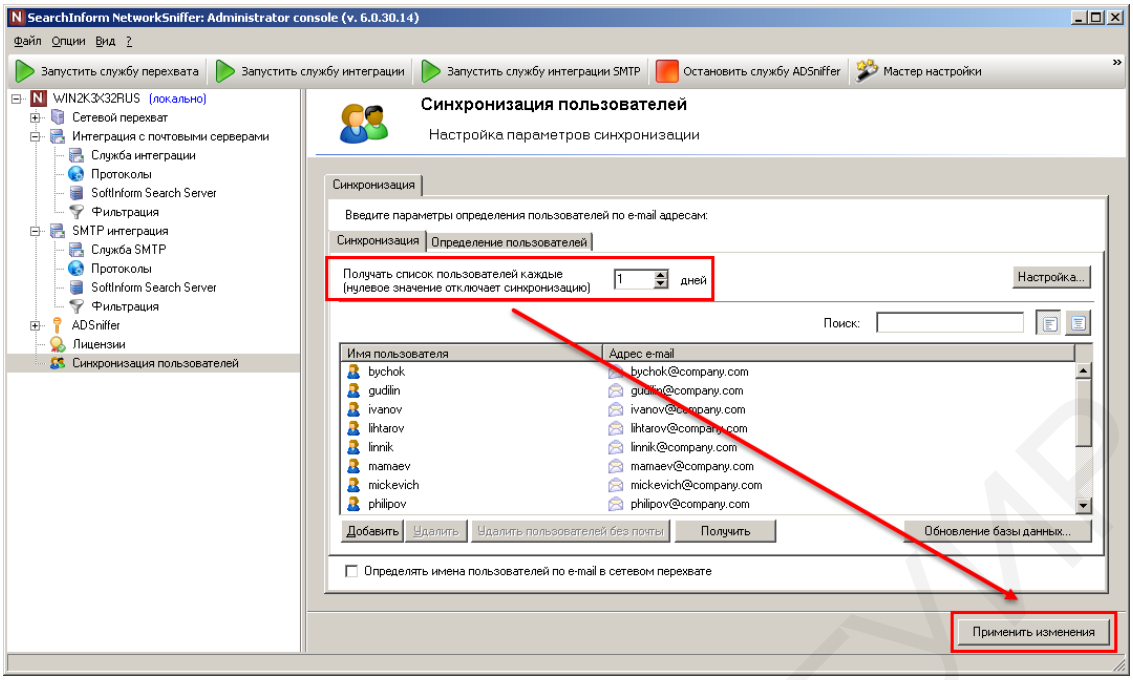


Рис. 2.30. Получение доменных имен из Active Directory

Привязка почтовых адресов и доменных имен вручную. Благодаря данной функции можно настроить привязки почтовых адресов пользователям, не добавленным в доступные каталоги Active Directory. Для этого необходимо нажать кнопку «Добавить» и в появившемся диалоговом окне ввести имя пользователя, после чего нажать «ОК» (рис. 2.31). Затем задать адрес электронной почты, соответствующий введенному имени.

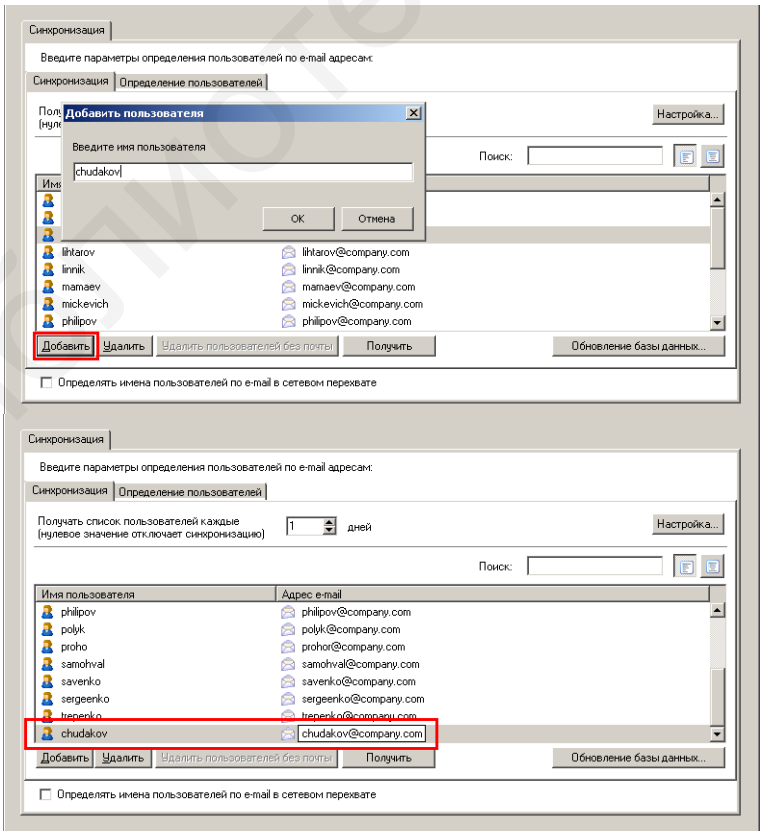


Рис. 2.31. Привязка почтовых адресов и доменных имен вручную

Библиотека БГУИР

Как уже было сказано ранее, если в результате проверки сообщения по привязкам почтовых адресов к доменным именам было найдено совпадение, сообщение отправляется на проверку по почтовым атрибутам. Если совпадения не было найдено, сообщения фильтруются по маскам адресов.

Фильтрация по маскам почтовых адресов является разрешающей. В случае совпадения сообщение записывается в базу. Для записи сообщения в базу достаточно совпадения по одному любому адресу – отправителя или получателя(ей).

Обрабатываемые адреса получателей и отправителей сообщений могут иметь форматы: petr.sidorov@company.com (простой почтовый адрес) или Петр Сидоров <petr.sidorov@company.com> (полный почтовый адрес с именем пользователя). Поэтому рекомендуется, чтобы маски электронных адресов начинались и заканчивались символом «*».

Примеры масок:

– *petr.sidorov@company.com*
– *@company.com*
– *petr.*@company*
– *petr.sidorov*
– *Петр Сидоров* (только для полного адреса с именем пользователя).

Для ввода масок необходимо выделить узел «Синхронизация» и перейти на вкладку «Определение пользователей», после чего нажать кнопку «Добавить» и ввести маску (рис. 2.32).

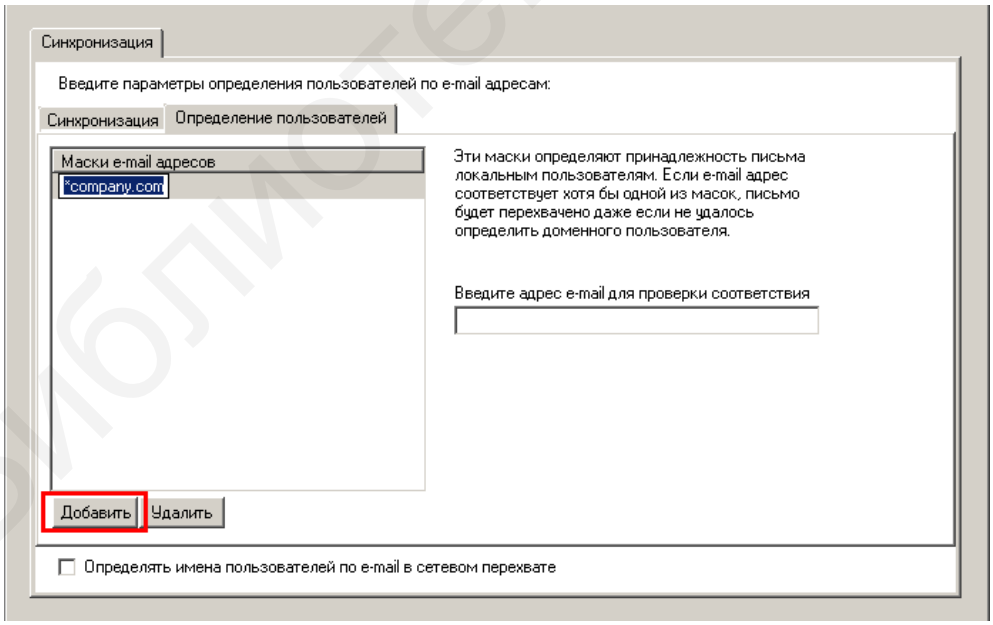


Рис. 2.32. Добавление маски

Для проверки корректности маски введите тестовый адрес электронной почты. Маски, удовлетворяющие введенному адресу, маркируются при помощи флажка (рис. 2.33).

Библиотека БГУИР

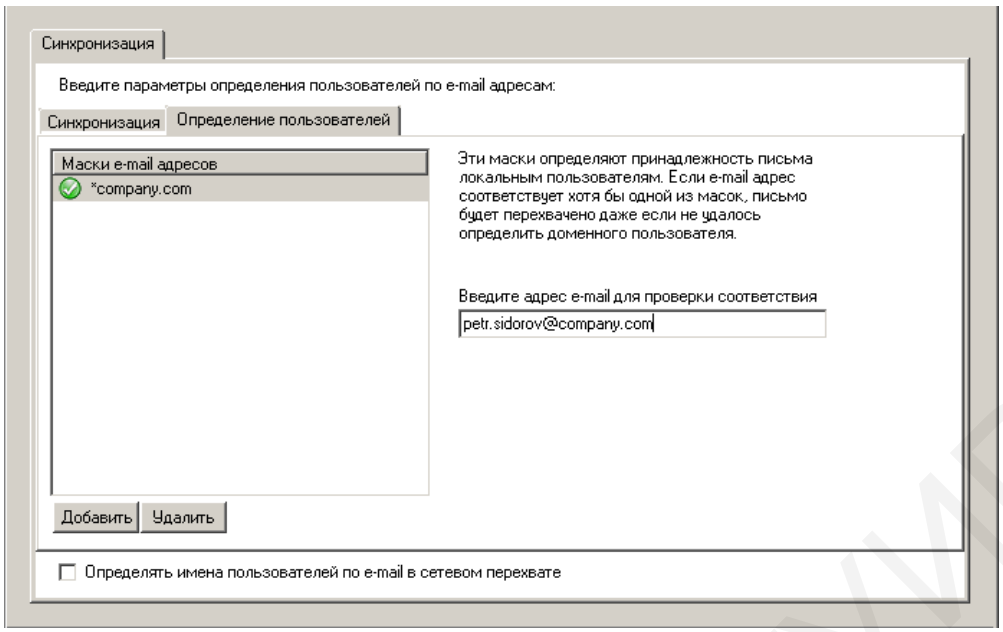


Рис. 2.33. Проверка корректности маски

Сообщения, которые не были записаны в базу данных после фильтрации по маскам почтовых адресов, в дальнейшем фильтруются по атрибутам сообщений.

Сообщения, которые предварительно выбраны (по привязкам или маскам почтовых адресов), проходят дополнительную проверку по атрибутам почтовых сообщений, подчиняясь при этом следующей логике:

– фильтры бывают разрешающими и запрещающими: если сообщение попадает под разрешающий фильтр, производится запись в базу данных; если сообщение удовлетворяет условиям запрещающего фильтра, сообщение не записывается в базу;

– проверку можно производить по следующим атрибутам фильтра: e-mail адрес (поля «От кого», «Кому»), доменное имя пользователя (определяется по привязкам почтовых адресов), тема письма, размер письма;

– фильтры имеют приоритет и проверяются последовательно в том порядке, в котором они заданы, до первого совпадения;

– строгий фильтр запоминает сработку (исключить/сохранить письмо) и запрещает отработку следующих за ним фильтров; нестрогий (обычный) фильтр запоминает сработавшее состояние и продолжает обработку следующих;

– если сообщение не попадает ни под одно условие, выполняется действие по умолчанию.

При настройке фильтров в электронных адресах рекомендуется использовать маски с символом «*», замещающим произвольный текст.

Фильтрация сообщений. Для настройки фильтров по атрибутам сообщений необходимо выделить узел «Фильтрация» в группе «Интеграция с почтовыми серверами» (рис. 2.34).

Библиотека БГУИР

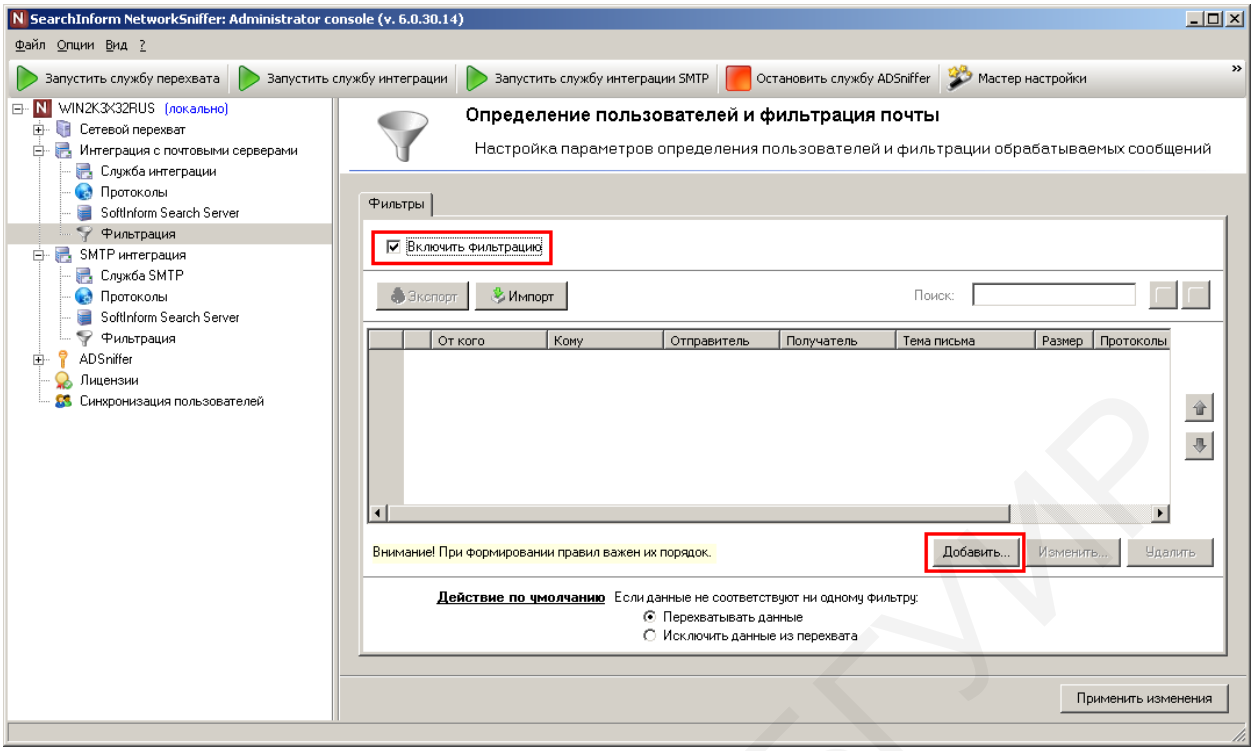


Рис. 2.34. Переход к настройке фильтров по атрибутам сообщений

Управление списком фильтров производится при помощи кнопок «Добавить» и «Удалить». Управление иерархией фильтров производится при помощи кнопок  и  . Для создания и настройки фильтра следует нажать кнопку «Добавить».

В открывшемся окне выбирается протокол, к которому будет применен фильтр, если для входящей и исходящей почты будут настраиваться отдельные фильтры и, соответственно, она будет сохраняться в разные индексы.

Также в рассматриваемой области указываются атрибуты фильтра при помощи предварительной установки соответствующих флажков. Рекомендуется, чтобы обрабатываемые доменные имена и адреса получателей/отправителей сообщений начинались и заканчивались маской с символом «*», подразумевающим любое количество и сочетание символов.

Чтобы выбрать доменные имена отправителей и/или получателей из списка, необходимо нажать кнопку  , в диалоговом окне «Выбор пользователя» – отметить соответствующего пользователя и подтвердить выбор кнопкой «Применить» (рис. 2.35). Если список пользователей достигает больших размеров, можно воспользоваться строкой поиска.

Библиотека БГУИР

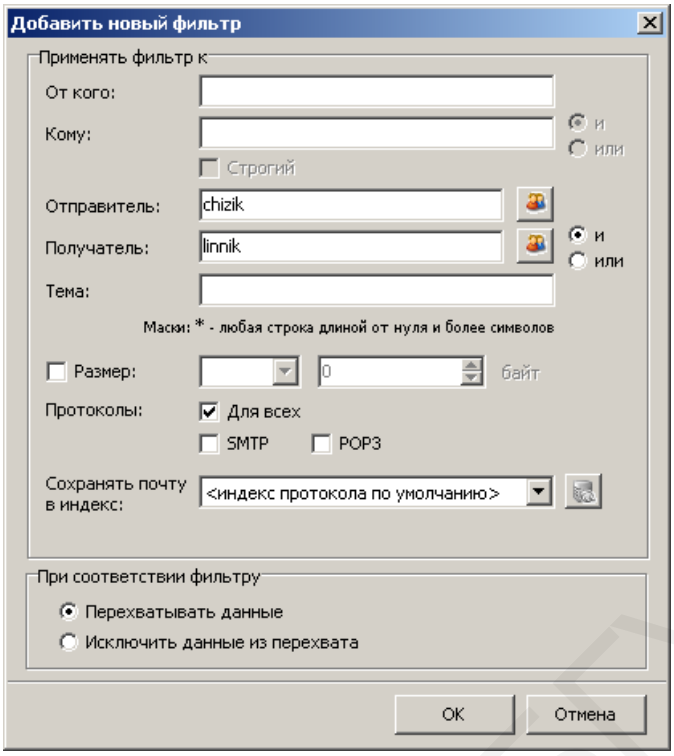


Рис. 2.35. Выбор доменных имен отправителей и/или получателей из списка

В случае когда в фильтре содержатся имена и отправителя, и получателя, с помощью переключателей «И/ИЛИ» указывается, должны ли совпадать оба имени при проверке по данному фильтру либо достаточно одного любого совпадения.

В нижней части информационного окна необходимо указать при помощи флажка, какой тип фильтра будет применен (разрешающий или запрещающий) при соответствии письма фильтру. При использовании разрешающего фильтра («Сохранить письмо») можно выбрать из выпадающего списка индекс, в который будет помещаться перехваченная почта.

При отметке параметра «Строгий» данный фильтр сработает, если условиям фильтра удовлетворяет хотя бы один адресат. Он сохранит/не сохранит документ в базу и запретит обработку всех следующих за ним фильтров. Нестрогий фильтр (при снятом флажке) сработает только в том случае, когда под условие одного или нескольких фильтров попадут все адресаты.

Кроме перечисленных операций следует указать действие по умолчанию в том случае, если письмо не будет соответствовать ни одному из фильтров (либо «Перехватывать данные», либо «Исключить данные из перехвата»). Пример заданных фильтров представлен на рис. 2.36.

Для осуществления поиска по списку заданных фильтров в поле «Фильтр» указывается значение атрибута, по которому будет производиться поиск, после чего в выпадающем списке выбирается сам атрибут. При этом в области фильтров отобразятся только фильтры, отвечающие введенному значению (если таковые имеются).

Библиотека БГУИР

Для сохранения и загрузки списка фильтров предусмотрены кнопки «Экспорт» и «Импорт» (поддерживаются форматы .lst, .txt и .csv).

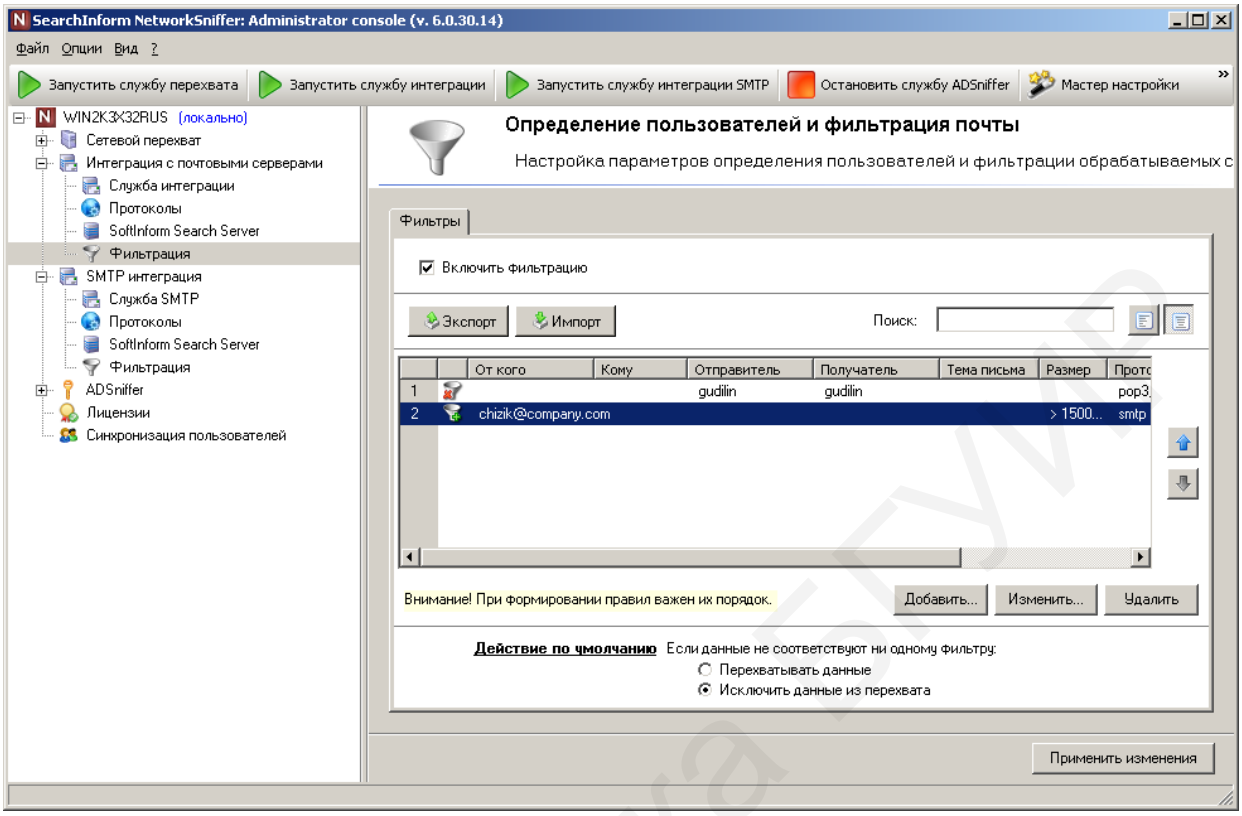


Рис. 2.36. Задание фильтров

2.3. Платформа SearchInform NetworkSniffer: особенности реализации контроля журналов событий Active Directory

Контроль и анализ событий журналов Active Directory позволяет выявлять подозрительные действия, которые могут совершаться системным администратором компании.

Служба ADSniffer мониторит изменения на контроллере домена и создает журнал изменений в собственной базе данных под управлением Microsoft SQL Server. В базу данных попадают только те события, которые представляют потенциальную угрозу безопасности системы, а именно:

– вход в систему, в том числе и неудачные попытки входа;

– выход из системы;

– создание/удаление учетной записи;

– изменения в учетной записи (сброс пароля, активация/деактивация);

– изменение членства учетной записи в группах;

– блокировка учетной записи при превышении допустимого количества попыток авторизации;

– очистка журнала безопасности на контроллере домена.

Библиотека БГУИР

Настройка параметров службы производится в узле «Служба ADSniffer».

Служба ADSniffer. Настройка параметров работы службы производится на вкладке «Параметры сервиса» узла «Служба ADSniffer» (рис. 2.37).

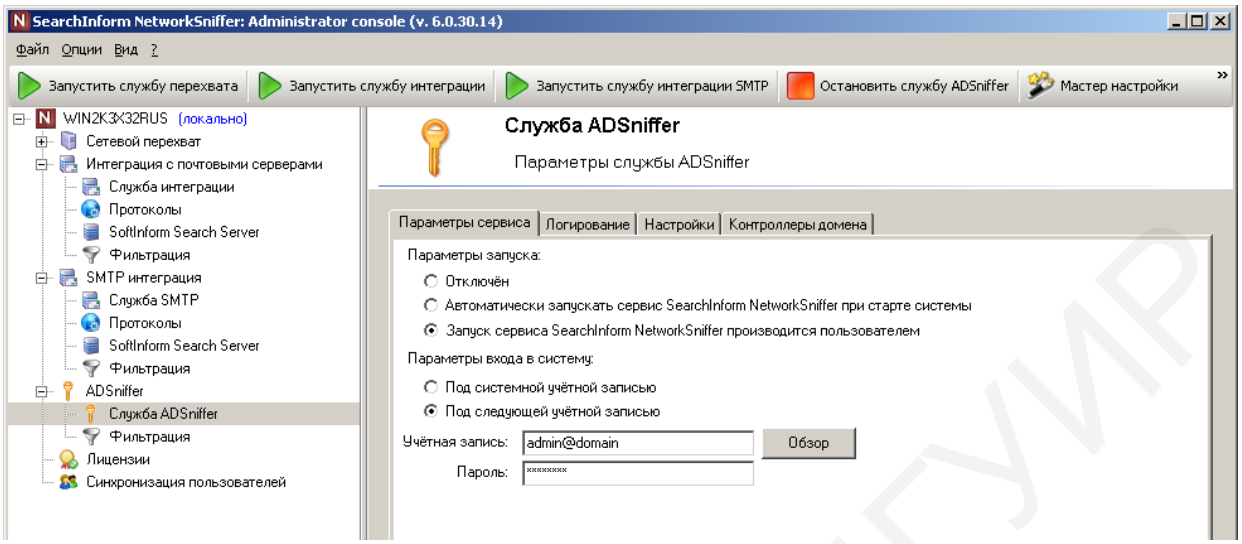


Рис. 2.37. Настройка службы

Обеспечены следующие возможности настройки службы:

– выбор типа запуска: «Автоматически», «Вручную», «Отключена»;

– выбор учетной записи, под которой будет работать служба.

Требования к учетной записи службы ADSniffer:

– возможность входа в качестве службы на сервере NetworkSniffer;

– право чтения журналов безопасности контроллера домена.

У системной учетной записи данные права отсутствуют.

Настройка уровня логирования на вкладке «Логирование». Протоколирование службы ADSniffer может потребоваться в целях проведения диагностики функционирования системы. Настройка уровня логирования производится в группе «Уровень логирования». Доступны следующие значения:

– «Обычный» – фиксируются серьезные ошибки службы ADSniffer и консоли управления сервером, повлекшие прерывание или аварийное завершение работы, запуск внутренних функций программы;

– «Детальный» – дополнительно фиксируется запуск внутренних функций программы в подробном виде; данный режим рекомендуется включать только по запросу сотрудников службы технической поддержки в случае критических проблем с сервером.

На вкладке «Настройка» задается база данных ADSniffer, в которую будут записываться «критичные» события из журналов безопасности. Подключение к контроллерам домена может производиться от разных учетных записей, для этого выберите узел «Служба ADSniffer» и перейдите на вкладку «Контроллеры домена».

Библиотека БГУИР

С помощью кнопки «Добавить контроллер домена» вызывается окно подключения к контроллеру домена, в котором задаются необходимые параметры. Для проверки подключения используется соответствующая кнопка (рис. 2.38).

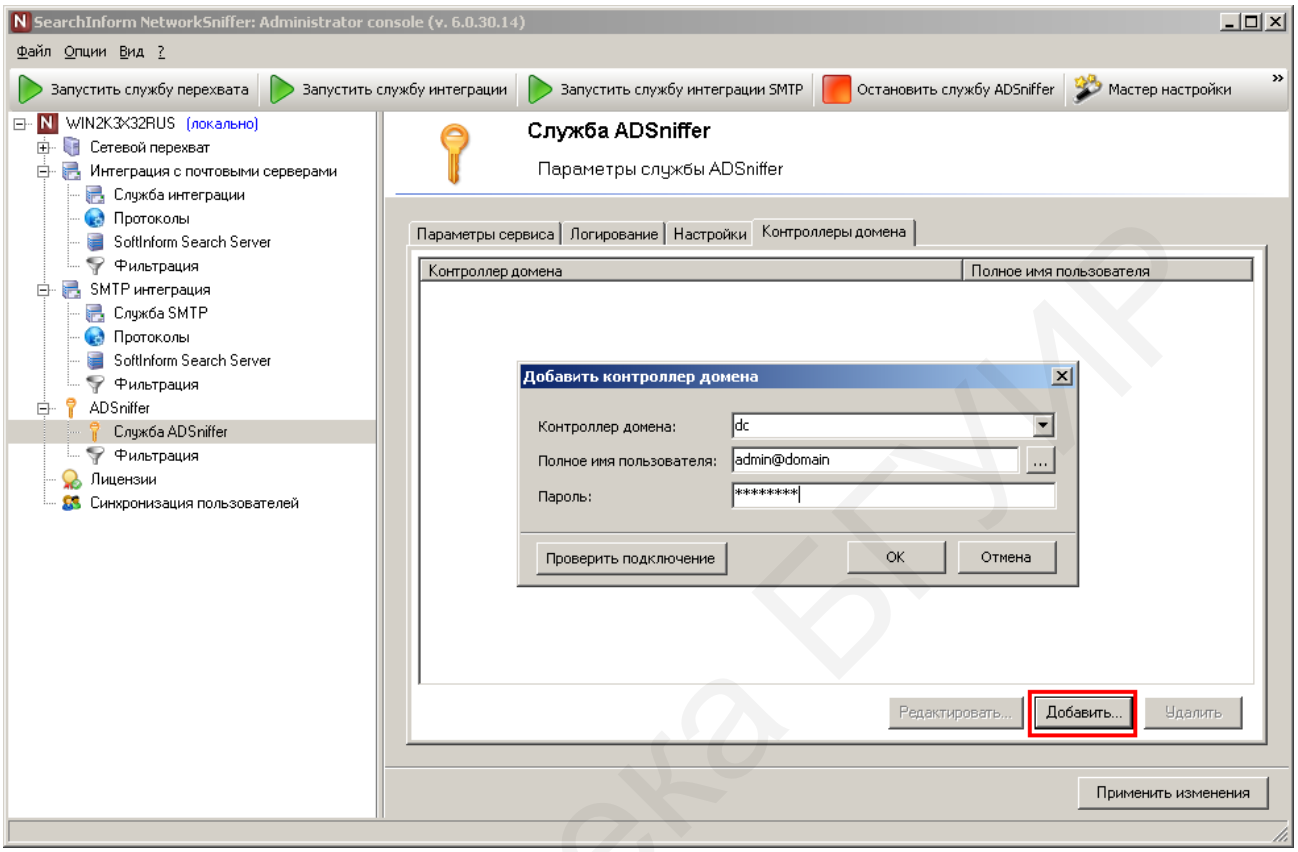


Рис. 2.38. Подключение к выбранному контроллеру домена

По завершении всех настроек нажмите «Применить изменения».

Фильтрация. NetworkSniffer позволяет настроить фильтры по пользователям, относительно которых требуется/не требуется осуществлять слежение за совершаемыми действиями на контроллерах домена и вносить информацию в собственную базу данных.

Фильтрация может потребоваться для следующих целей:

– отмена мониторинга заданных пользователей;

– приведение параметров в соответствие лицензии.

Для добавления фильтров необходимо выделить узел «Фильтрация» в группе «Служба ADSniffer» (рис. 2.39).

Библиотека БГУИР

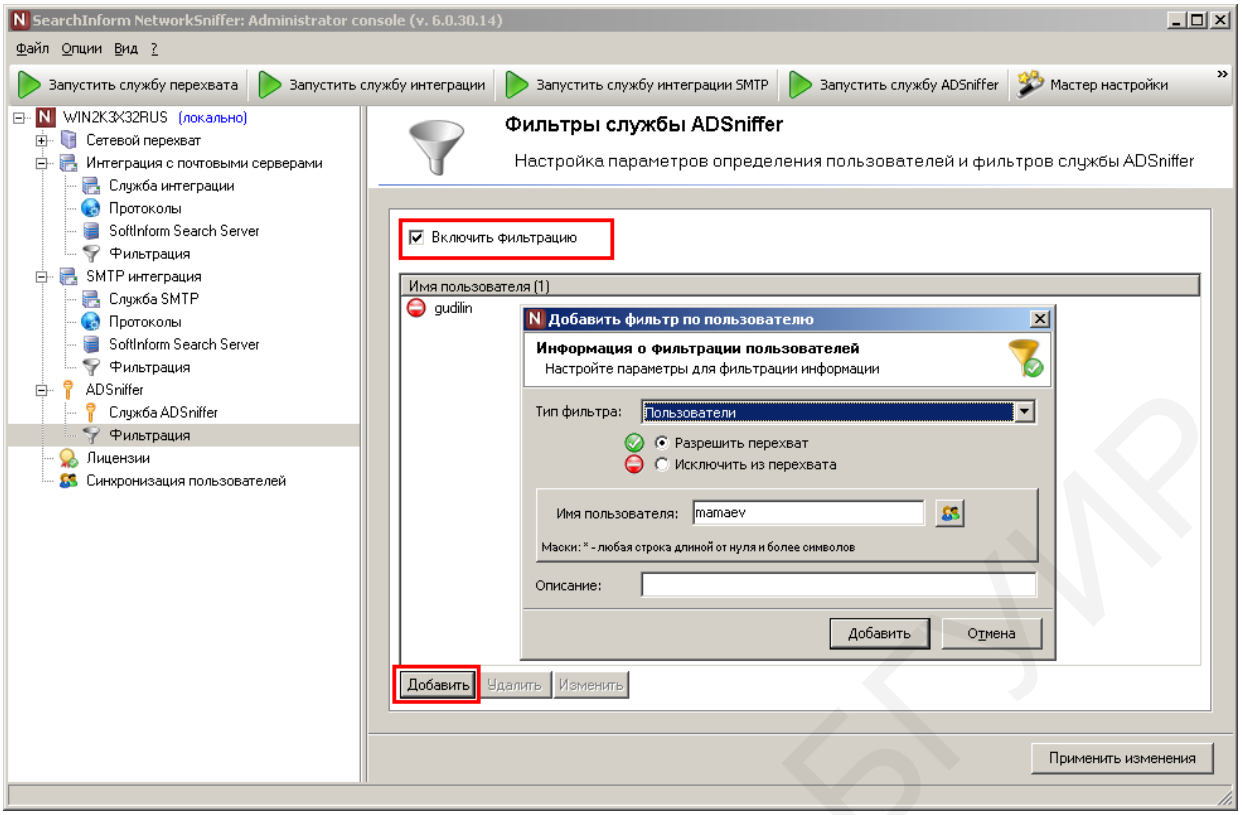


Рис. 2.39. Добавление фильтра

Для включения режима фильтрации необходимо отметить соответствующий чекбокс. Нажмите кнопку «Добавить» для создания фильтра. Выберите разрешающий/запрещающий тип фильтрации, отметьте необходимых пользователей и нажмите «Добавить». По завершении всех настроек нажмите «Применить изменения».

2.4. Платформа SearchInform EndpointSniffer: особенности реализации агентского перехвата трафика

Общая характеристика и принцип работы платформы SearchInform EndpointSniffer [4]. Платформа SearchInform EndpointSniffer предназначена для перехвата трафика пользователей, извлечения из него информации, записи собранной информации в базу данных и поиска по ней. В отличие от серверного модуля NetworkSniffer перехват производится не на уровне сетевых шлюзов, а на уровне рабочих станций сети при помощи установленных на них агентов. Перехват осуществляется в невидимом для пользователей режиме.

Перечень ключевых функций EndpointSniffer.

1. Перехват отправленных/полученных пользователями данных, к числу которых относятся:

– данные, передаваемые на внешние устройства;

– история операций с файлами, расположенными на файл-серверах или рабочих станциях;

Библиотека БГУИР

– файловые документы, отправленные или полученные по FTP-соединению;

– мгновенные сообщения, переданные по протоколам Gadu-Gadu, OSCAR (службы ICQ, AIM), MMP (Mail.ru Agent), MSNP (Windows Live/MSN), XMPP (Google Hangouts, Jabber);

– сообщения и файлы, отправленные при помощи браузера;

– сообщения электронной почты, отправленные или полученные по протоколам SMTP, POP3, IMAP, MAPI (MAPI и RPC over HTTP), NNTP, а также протоколы веб-почты под условным названием Web mail:

- EWS (Exchange Web Services) – исходящая и входящая почта;
- KOC (Kerio Outlook Connect) – исходящая и входящая почта;
- OWA (Outlook Web App и Outlook Web App Light) – исходящая почта;
- Zimbra Web Client – исходящая почта;

– другие почтовые веб-сервисы – исходящая и входящая почта;

– запись речи сотрудников;

– скриншоты экранов мониторов рабочих станций пользователей;

– документы, отправленные на печать с помощью физических и виртуальных принтеров;

– текстовые и голосовые сеансы связи по Skype, файлы и SMS-сообщения, переданные или полученные при помощи Skype;

– текстовые и голосовые сеансы связи по Microsoft Lync, а также файлы, переданные или полученные при помощи MS Lync;

– текстовые и голосовые сеансы связи по Viber Desktop, файлы, переданные или полученные при помощи Viber Desktop, а также списки контактов;

– данные об активности приложений, запускаемых пользователями;

– входящие и исходящие данные облачных сервисов (Google Docs, OneDrive, Office 365, Dropbox, Evernote, Яндекс Диск, cloud.mail.ru), файлы, передаваемые при помощи MS SharePoint;

– данные, передаваемые с помощью мобильных устройств на базе iOS.

2. Перехват данных, переданных через зашифрованное SSL-соединение.

3. Шифрование данных, записываемых на USB Flash.

4. Запись перехваченных данных в базу под управлением Microsoft SQL Server или в файловое хранилище.

5. Присвоение перехваченным документам атрибутов – даты и времени перехвата, домена, доменного имени, IP- и MAC-адресов, специфических пользовательских данных (логин Skype, почтовые адреса, имя принтера, число отправленных на печать страниц и др.).

6. Создание индексов, предназначенных для анализа перехваченных данных и контекстного поиска, из консоли администрирования EndpointSniffer.

7. Хранение всех настроек и журналов событий сервера в базе данных Microsoft SQL.

Библиотека БГУИР

Принцип работы SearchInform EndpointSniffer. На рабочие станции локальной сети устанавливаются агенты, обеспечивающие перехват пользовательской информации и ее передачу на сервер управления (рис. 2.40).

Сервер управления записывает перехваченные данные (сообщения электронной почты и сервисов мгновенных сообщений, сеансы связи Skype, скриншоты экранов мониторов рабочих станций пользователей и т. п.) в базу под управлением СУБД Microsoft SQL Server. Запись данных, переданных на внешние устройства, а также данных, переданных по протоколу FTP, производится не в базу данных, а в файловое хранилище. Перехват можно ограничить по пользовательским атрибутам (пользователю домена, IP- и MAC-адресу).

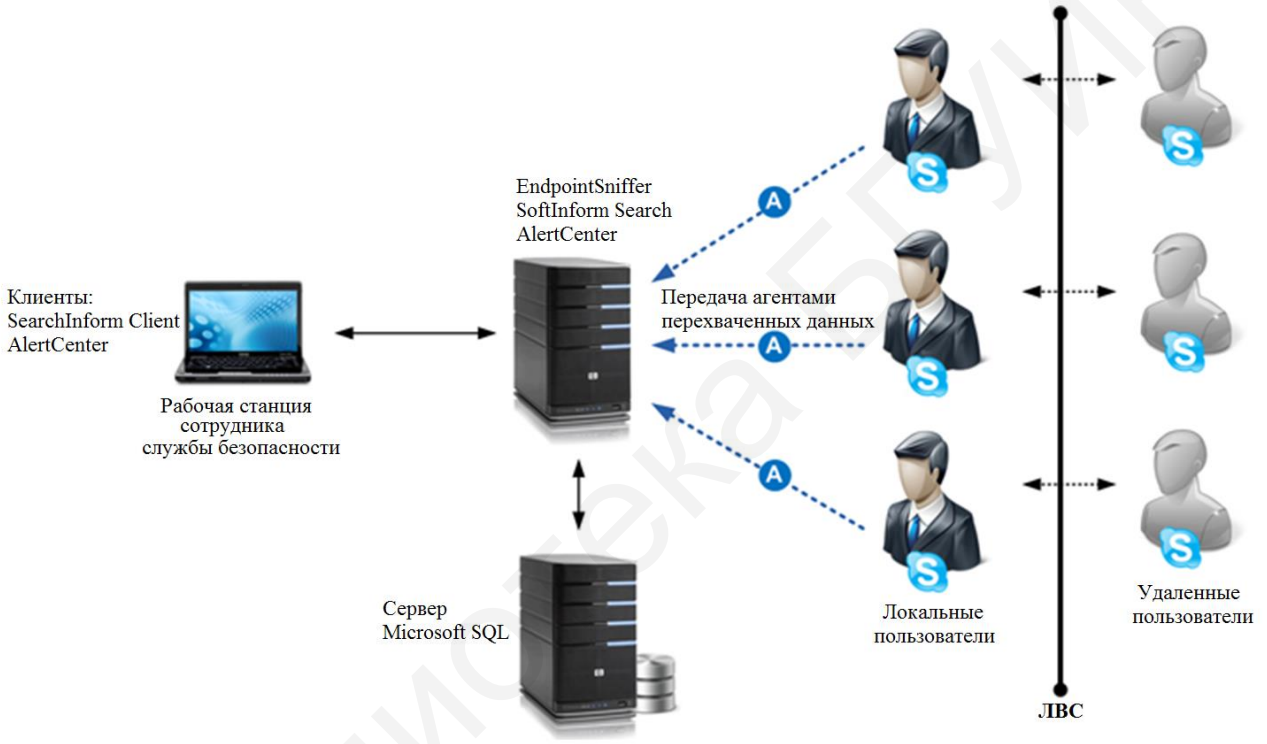


Рис. 2.40. Схема работы SearchInform EndpointSniffer

Для быстрого поиска и просмотра документов база данных/хранилище индексируется сервером SoftInform Search. Благодаря реализованной функции обновления индексов согласно заданному расписанию обеспечивается поддержание индексов в постоянно актуальном состоянии.

Для автоматизации проверок и уведомлений используется приложение AlertCenter. По заданному расписанию AlertCenter опрашивает подключенные индексы по списку критериев поиска и автоматически высылает администратору уведомления в случае обнаружения инцидентов.

Для просмотра документов, отвечающих поисковому запросу, применяется клиентское приложение SearchInform Client. Клиент обеспечивает просмотр истории активности пользователей с возможностью фильтрации по атрибутам документов.

Библиотека БГУИР

Консоль администратора SearchInform EndpointSniffer. Управление серверной частью платформы осуществляется при помощи консоли (рис. 2.41).

Для доступа к настройкам консоли администрирования служит кнопка «Настройки программы...», а также одноименная команда в меню «Опции».

В левой части консоли в виде дерева располагаются обозначения имеющихся в консоли узлов:

– «Сервер» (отображается как имя сервера) – для пуска сервиса обработки данных;

– «Сетевое окружение» – для управления агентами на рабочих станциях;

– «Агенты» – для настройки баз и хранилищ, в которые помещаются перехваченные данные, а также для дополнительных настроек агентов (DeviceSniffer, FileSniffer, HTTPsniffer, IMSniffer, MailSniffer, MonitorSniffer, SkypeSniffer) и включения режима остановки почты, отправляемой по протоколу SMTP;

– «Текущая активность» – для отображения текущих заданий сервера;

– «SoftInform Search Server» – для создания индексов и управления ими;

– «Лицензия» – для управления лицензией на использование продукта;

– «Фильтры» – для настройки параметров фильтрации документов по атрибутам пользователей;

– «Исключения (системные)» – для исключения из обработки агентами системных процессов;

– «Исключения (пользовательские)» – для исключения из обработки агентами отдельных пользовательских приложений и хостов;

– «SSL-соединения» – для просмотра журнала соединений SSL.

В правой части консоли располагается окно просмотра. Для перехвата информации на целевые станции должны быть установлены агенты с подключенными модулями обработки протоколов – модулями перехвата. В настоящее время используются следующие модули перехвата: Device, File, FTP, HTTP, IM, KeyLogger, Mail, Microphone, Monitor, Print, Activity Monitor, Skype, Cloud, Lync, Viber. Перед установкой агентов на рабочие станции пользователей брандмауэр Windows на сервере EndpointSniffer должен быть выключен либо в нем должны быть прописаны исключения на работу служб EndpointSniffer.

Также необходимо удостовериться, что в настройках EndpointSniffer («Настройки программы» → «Установка агентов» → «Новые агенты») флажок в строке «Запретить установку новых агентов» снят. В противном случае агенты не смогут быть установлены.

Библиотека БГУИР

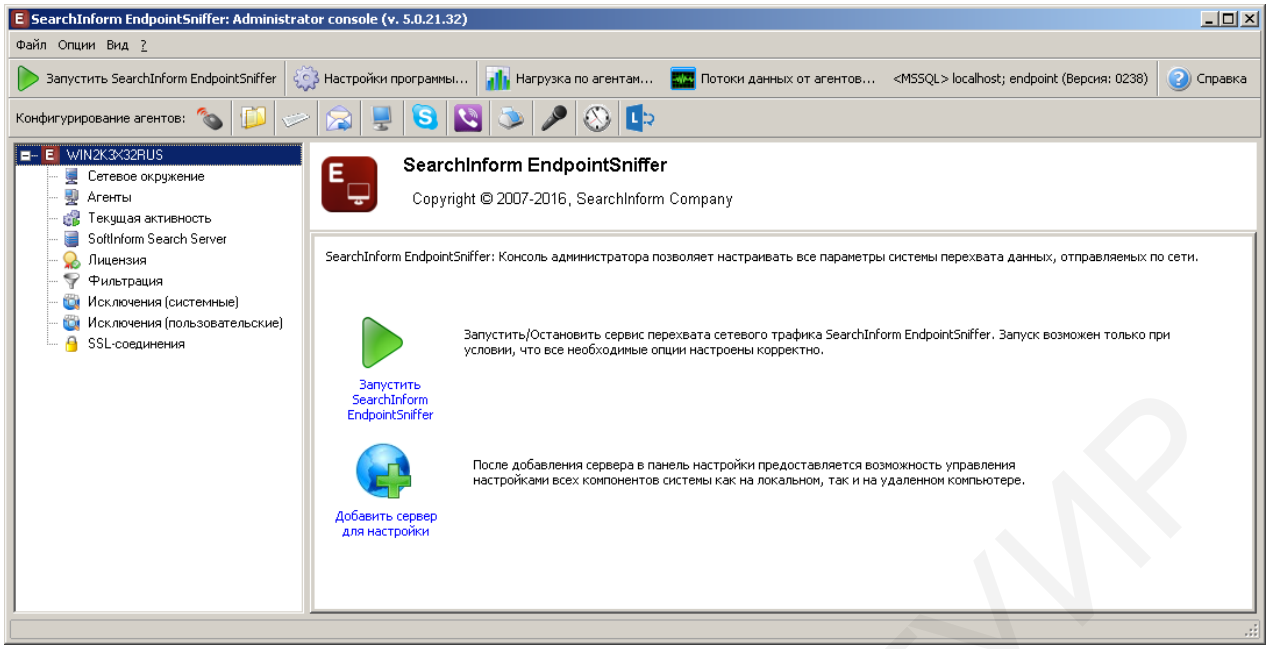


Рис. 2.41. Консоль администратора SearchInform EndpointSniffer

Управление агентами на рабочих станциях производится на вкладке «Сетевое окружение». Операции установки и удаления агентов можно производить как с отдельными компьютерами, так и с целыми группами.

Выбор рабочих станций для установки агентов. С помощью раскрывающегося списка необходимо выбрать один из трех типов конфигурации сетевого окружения EndpointSniffer:

– «Группы и компьютеры» – список всех компьютеров, организованный по группам Active Directory;

– «Только компьютеры» – простой список всех компьютеров;

– «Только компьютеры с агентами» – простой список компьютеров, на которые установлены агенты (данный режим не подходит для установки агентов на новые компьютеры);

– «Пользовательский режим» – настраиваемый список групп.

Сервер EndpointSniffer получает список компьютеров из каталога Active Directory. Также списки компьютеров и групп можно импортировать.

При большом количестве компьютеров в списке можно воспользоваться поисковыми фильтрами. При вводе первых символов запроса список компьютеров сокращается, отображая лишь те, по которым имеются соответствия запроса.

Для применения и сохранения текущей конфигурации служит кнопка «Переконфигурирование», которая используется в редких случаях и в основном специалистами по обслуживанию и поддержке системы безопасности. Для сохранения настроенного списка компьютеров используется операция экспорта.

На рис. 2.42 представлен пример порядка выбора рабочих станций для установки агентов.

Библиотека БГУИР

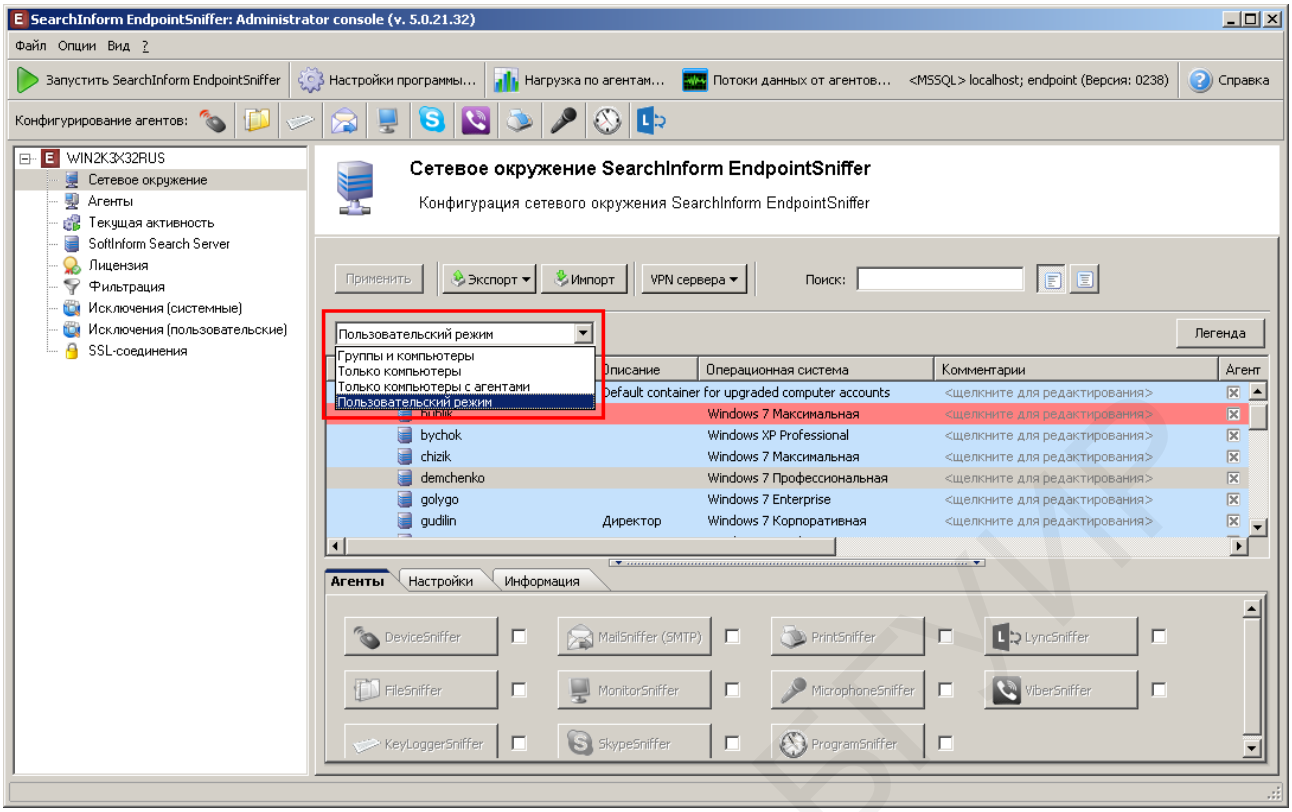


Рис. 2.42. Выбор рабочих станций для установки агентов

Для установки агентов необходимо выделить требуемые группы или рабочие станции и установить флажки для отслеживаемых каналов передачи данных. Также можно щелкнуть правой кнопкой мыши и воспользоваться контекстным меню (команда «Инсталлировать»). Для установки всех протоколов на выбранные компьютеры предусмотрена команда «Инсталлировать» → «Все» (рис. 2.43). Для подтверждения настроек необходимо нажать кнопку «Применить».

После этого в течение некоторого времени будет происходить установка агентов и модулей перехвата. Установленные модули перехвата отображаются при помощи маркера . Компьютеры, на которые установлены агенты или модули перехвата, будут подсвечены бледно-голубым цветом. Также будут подсвечены группы, в которых есть хотя бы одна рабочая станция с установленным агентом. Для запуска установленных агентов следует применить флажок в столбце «Агент» для целевых рабочих станций и нажать кнопку «Применить».

Колонка «Состояние» в окне просмотра свидетельствует об активности/неактивности установленного агента:

– значок – агент установлен и запущен (происходит перехват данных);

– значок – агент установлен, но не запущен (перехват данных не происходит).

Процедура установки агентов средствами групповых политик производится на контроллере домена.

Библиотека БГУИР

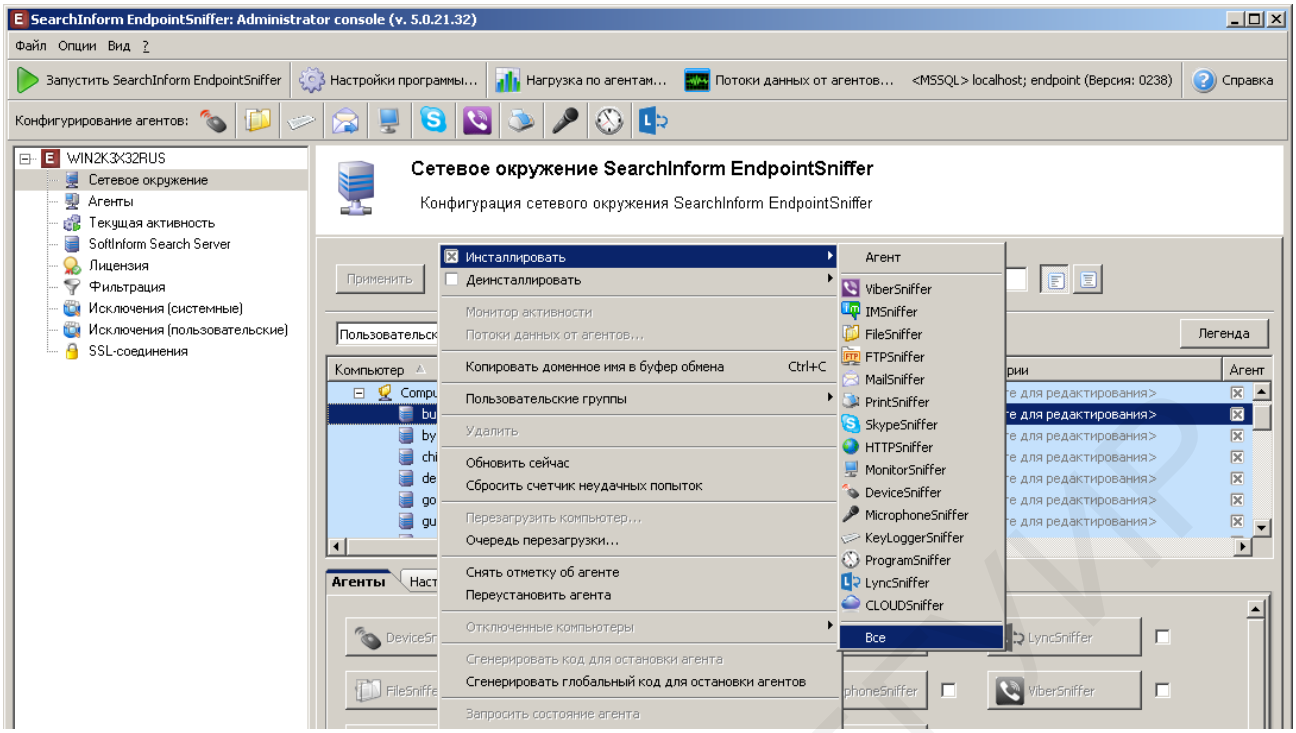


Рис. 2.43. Установка агентов

MSI-дистрибутив агента должен быть помещен в сетевую папку, доступную с контроллера домена. Требуемый MSI-пакет хранится в следующих папках:

– c:\Program Files(x86)\SearchInform\SearchInform EndpointSniffer\service\ESClient.msi – для 64-разрядных операционных систем;

– c:\Program Files\SearchInform\SearchInform EndpointSniffer\service\ESClient.msi – для 32-разрядных операционных систем.

Политику принудительной установки агентов можно привязывать к пользователям и компьютерам. В случае привязки политики к пользователям установка агента будет произведена только при следующем входе пользователя в систему, поэтому рекомендуется привязывать политику к компьютерам.

Для установки агентов предусмотрена определенная последовательность действий:

1. В оснастке «Редактор объектов групповой политики» открыть «Конфигурация пользователя» → «Конфигурация Windows» → «Сценарии (вход/выход из системы)» (рис. 2.44). В случае привязки к компьютеру – «Конфигурация компьютера» → «Конфигурация Windows» → «Сценарии (запуск/завершение)».

2. Далее открыть окно свойств «Вход в систему» и нажать кнопку «Добавить», после чего настроить запуск установщика msiexec со следующими параметрами (рис. 2.45): -i \\SERVER\install\ESClient.msi ADDLOCAL=all SIHOST=ESServer:80:0:simh REBOOT=ReallySuppress -quiet -L*v c:\install.log< /FONT>.

Здесь:

– -i – параметр запуска установщика;

– \\SERVER\install\ESClient.msi – сетевой путь к MSI-пакету установщика агента;

– ADDLOCAL=all – параметр добавления агентов;

– REBOOT=ReallySuppress – параметр, запрещающий принудительную перезагрузку, необходимую при обновлении «занятых» файлов;

– -quiet – параметр установки агента в невидимом режиме;

– -L*v \\SERVER\install\%COMPUTERNAME%_install.log – параметр логирования процесса установки агентов;

– SIHOST=ESServer:80:0:simh – параметр, указывающий на имя или IP-адрес сервера и порт, по которому передается информация (Пример для IP-адреса: SIHOST=192.168.20.1:80:0:simh. При этом не следует изменять параметр 0:simh!).

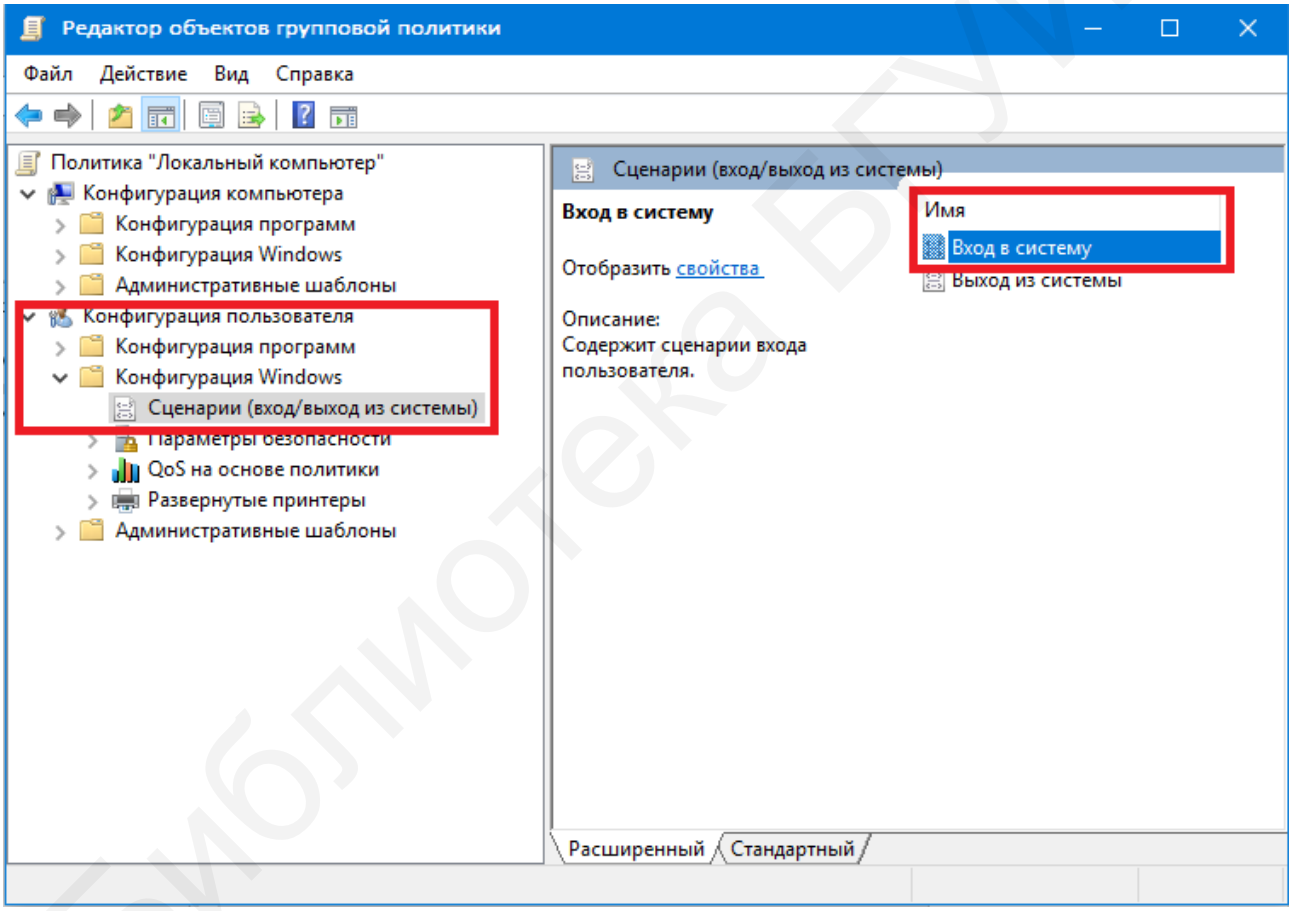


Рис. 2.44. Установка агентов средствами групповых политик

3. Добавить сценарий в политику «Вход в систему» (рис. 2.46).

4. Выполнить команду gpupdate /force для обновления политики (рис. 2.47).

Библиотека БГУИР

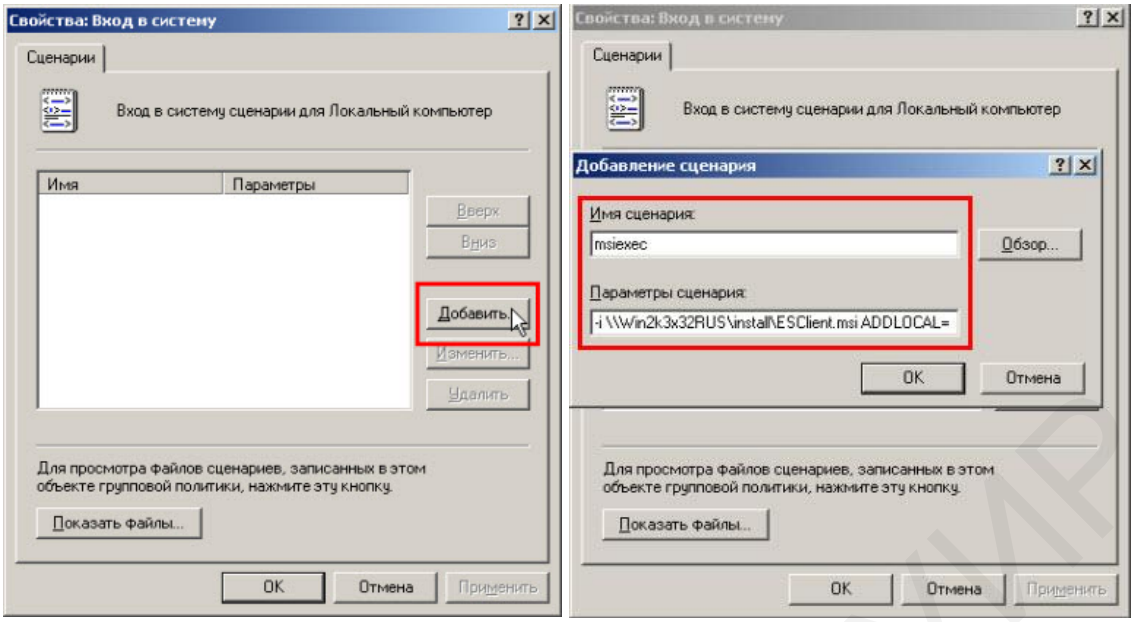


Рис. 2.45. Настройка запуска установщика

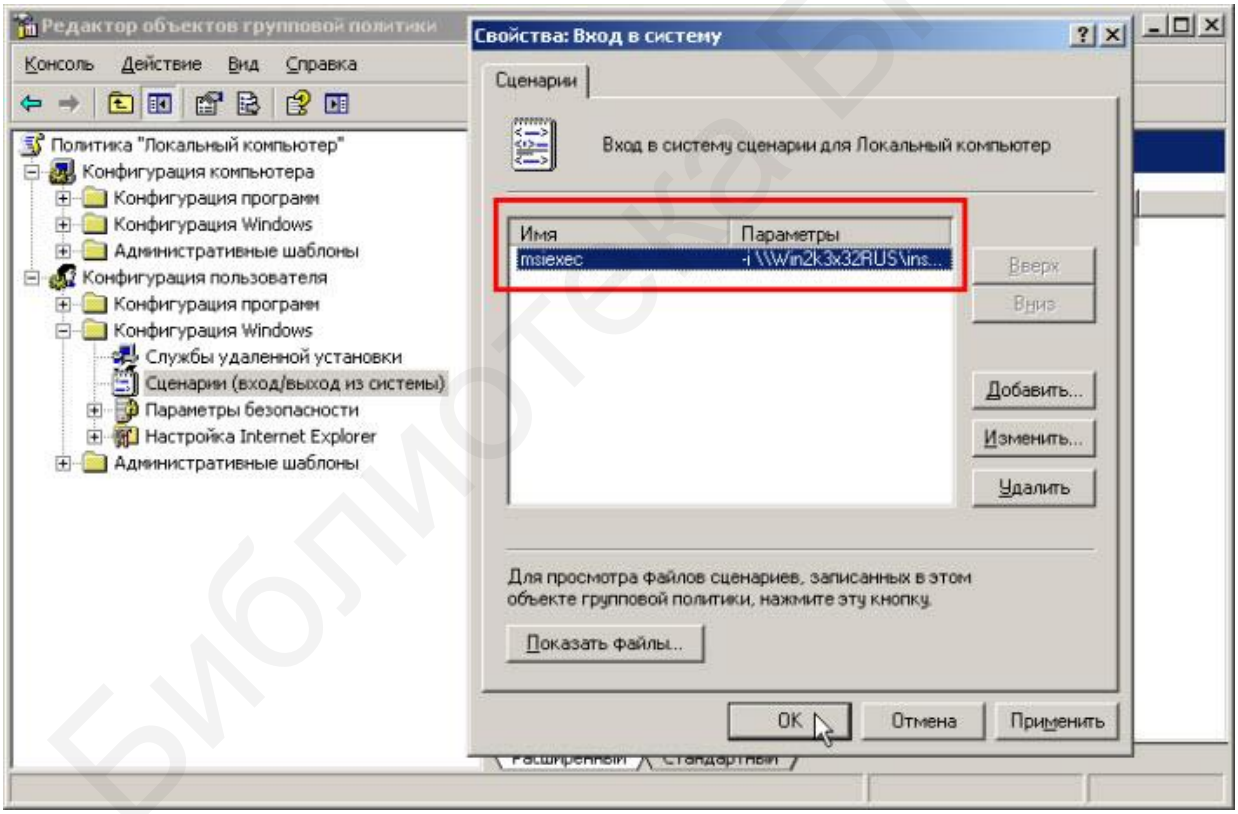


Рис. 2.46. Добавление сценария в политику «Вход в систему»

Библиотека БГУИР

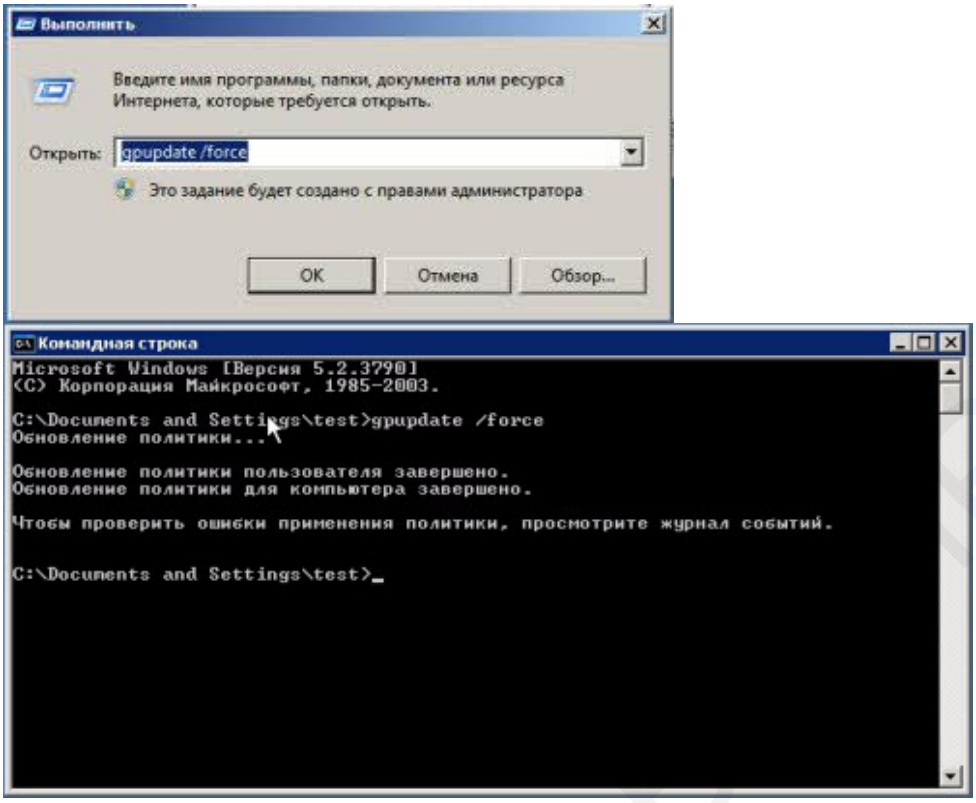


Рис. 2.47. Выполнение команды gpupdate /force

Также установку агентов можно осуществить и вручную. Для этого необходимо скопировать дистрибутив агента в папку на целевую рабочую станцию и запустить дистрибутив из командной строки: msiexec.exe -i ESClient.msi ADDLOCAL=all SIHOST=192.168.20.1:80:0:simh SIDEBUG=1 -qn -L*v install.log.

Здесь:

– msiexec.exe – установщик Windows;

– -i – параметр запуска установщика;

– ESClient.msi – MSI-дистрибутив агента;

– ADDLOCAL=all – параметр добавления агентов;

– SIHOST=192.168.20.1:80:0:simh – параметр, указывающий на имя или IP-адрес сервера и порт, по которому передается информация;

– SIDEBUG = 1 (допускается SIDEBUG=0) – параметр включения/отключения логирования;

– L*v – параметр логирования процесса установки агентов;

– install.log – имя лог-файла.

Индивидуальная настройка агентов. Для рабочих станций пользователей можно задавать индивидуальную конфигурацию. Их настройка производится на вкладках, расположенных в правой нижней части узла «Сетевое окружение». Вкладка «Агенты» позволяет осуществить настройку модулей перехвата для отдельной рабочей станции (рис. 2.48).

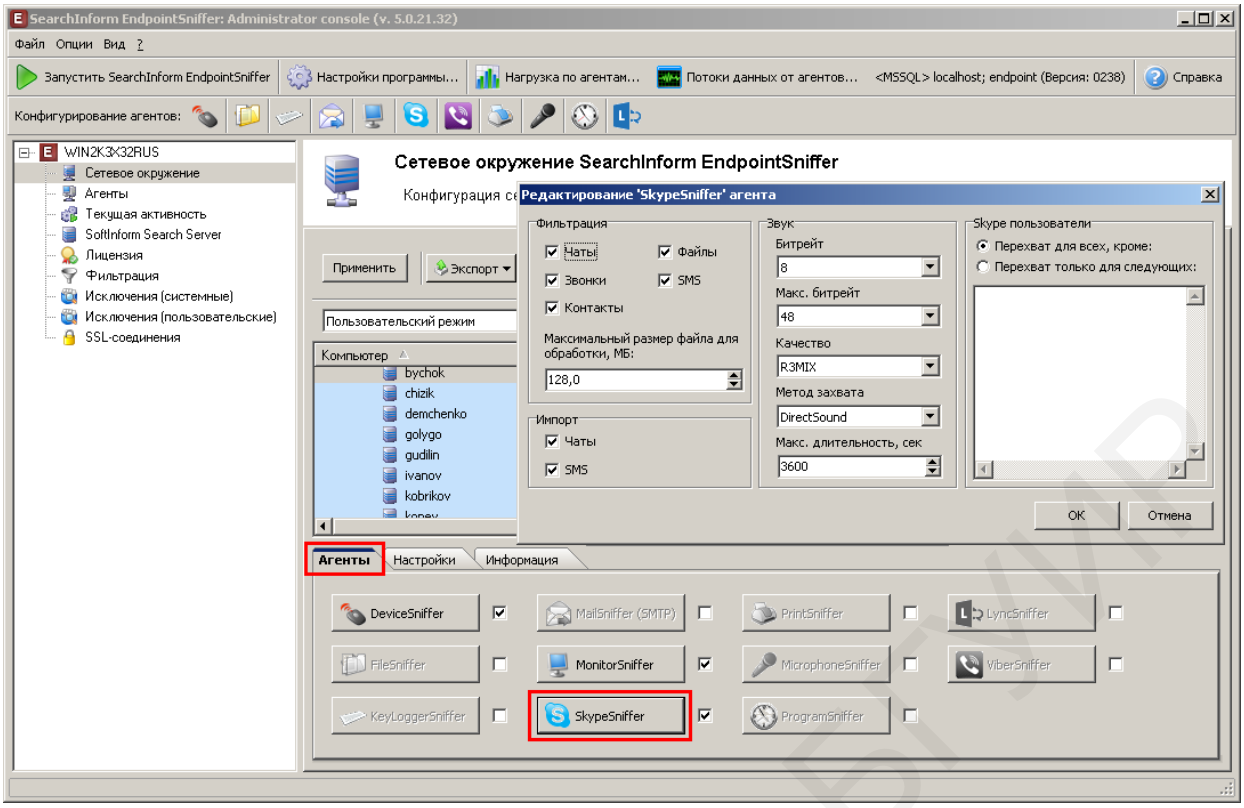


Рис. 2.48. Настройка SkypeSniffer для отдельной рабочей станции

Настройки могут быть глобальными (общими для всех пользователей системы), групповыми (назначенными для какой-либо определенной группы пользователей) и пользовательскими (индивидуальными для каждого пользователя). Они представляют собой иерархическую структуру: например, групповые настройки могут переопределять глобальные, которые являются для них родительскими, а пользовательские настройки перекрывают в свою очередь и глобальные, и групповые, наследуя их параметры как основу и перекрывая их своими индивидуальными значениями.

Задать индивидуальные настройки можно как для одного компьютера, так и для группы. Переопределение производится при задании настроек компьютеру/группе, как показано на рис. 2.49.

На вкладке «Общее» вкладки «Настройки» (рис. 2.50) отображается следующее.

1. Параметры использования дискового пространства:

а) максимальный размер очереди – максимальный объем дискового пространства (в мегабайтах), зарезервированного для записи временных данных; по достижении указанного значения агент для сохранения новых данных будет удалять наиболее старые;

б) минимальное свободное место на диске – минимальный объем свободного дискового пространства (в мегабайтах); если свободного дискового пространства недостаточно, то агент будет производить перезапись старых данных вне зависимости от параметра «Максимальный размер очереди».

Библиотека ВГУИР

2. Режим блокировки исходящей почты (может использоваться в случае отсутствия доступа к серверу; для блокировки почты должен быть установлен флажок в строке «Блокировать SMTP, когда сервер ES недоступен»):

а) флаг «Остановка записи данных при переполнении хранилища» – используется для прекращения записи при переполнении хранилища данных;

б) флаг «Скрывать присутствие агентов в системе» – позволяет включать/отключать режим невидимости агентов; по умолчанию работающие агенты отображаются в окне «Диспетчер задач» Windows и в оснастке «Службы» рабочей станции; в дополнение к этому файлы агентов по умолчанию отображаются в папке %PROGRAMFILES%\SearchInformAgent\SIFilter_x.x.x.x\, где x.x.x.x – текущая версия серверного модуля, например, 5.0.17.26; режим невидимости агентов можно включить при помощи консоли администрирования; в данном режиме происходят следующие изменения: служба агента не отображается в окне «Диспетчер задач»; служба агента не отображается в оснастке «Службы»; папка агента становится невидимой;

в) флаг «Удаление агентов после перезагрузки» – включает/отключает опцию «Удаление агентов после перезагрузки».

3. Опция «Сертификат» (задается имя корневого SSL-сертификата (имя по умолчанию – «Generic Root CA»); после изменения имени создается новый сертификат с собственным уникальным ключом, который добавляется во все хранилища; старый сертификат в дальнейшем не используется).

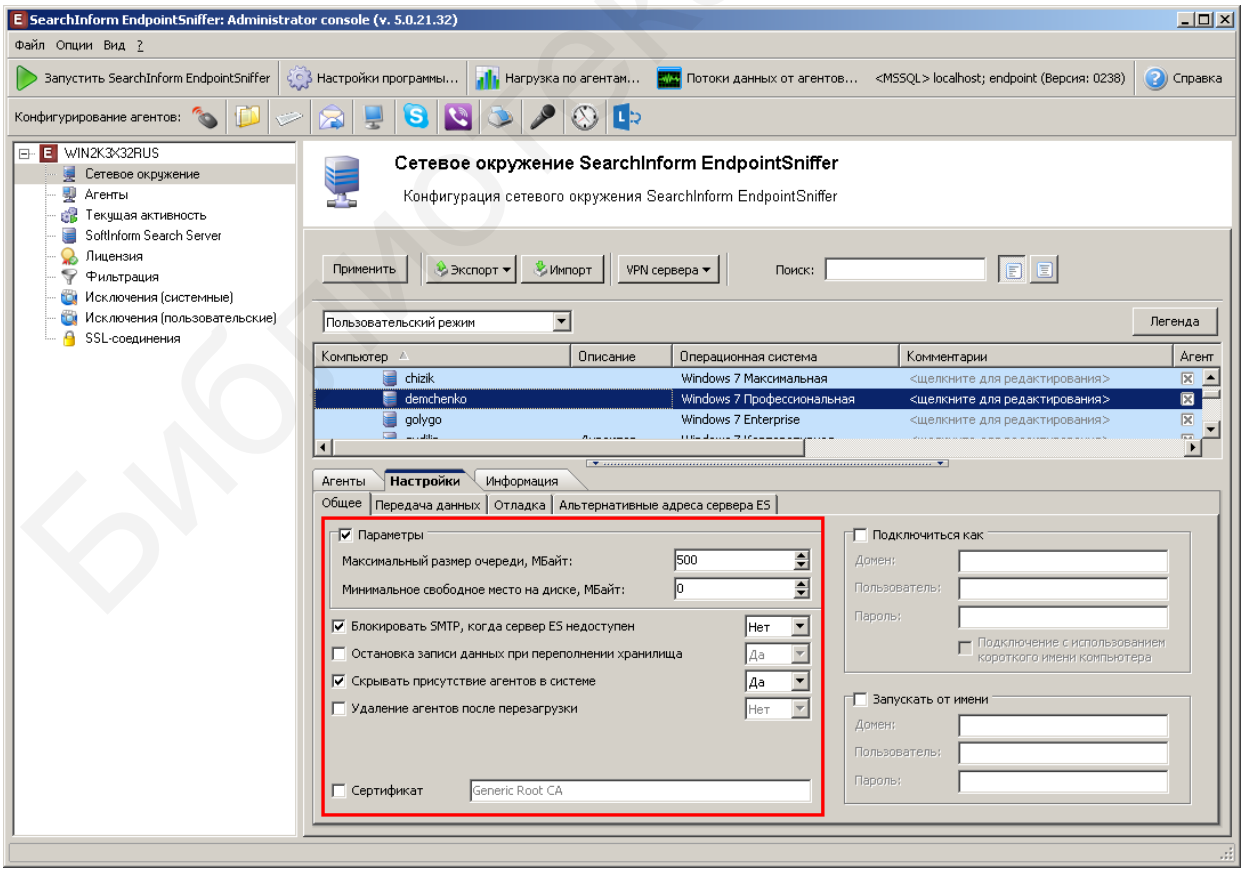


Рис. 2.49. Переопределение родительских настроек

Библиотека БГУИР

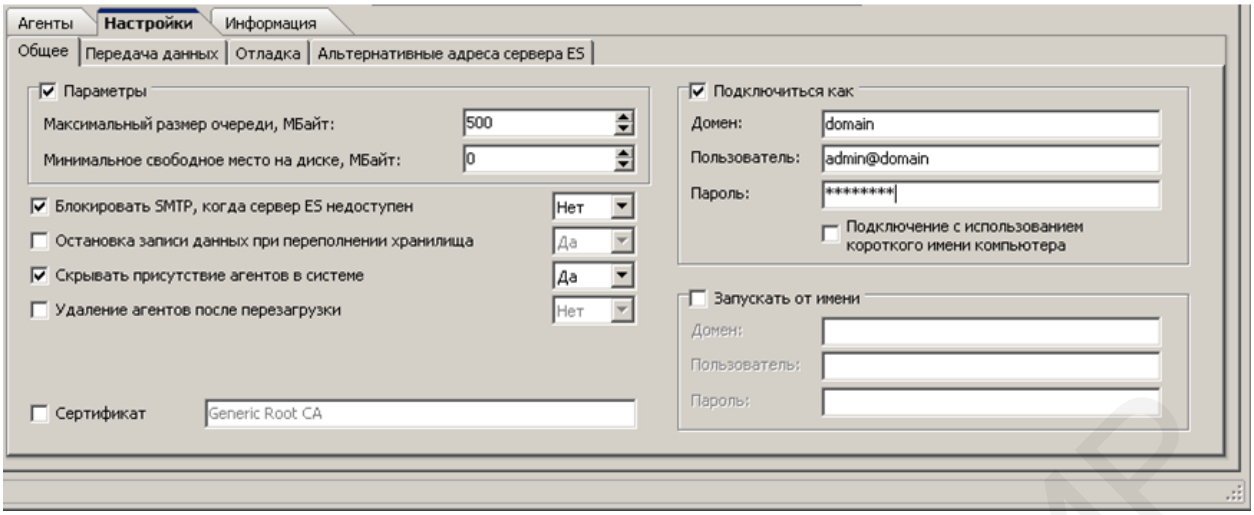


Рис. 2.50. Вкладка «Общее»

По умолчанию установка агентов EndpointSniffer выполняется под системной учетной записью. При необходимости учетная запись, под которой выполняется установка агента на выбранную рабочую станцию, может быть изменена (например, при нехватке прав у текущей учетной записи для установки агента на рабочей станции, находящейся в другом домене). Настройка учетной записи производится на вкладке «Подключиться как».

Флажок в строке «Подключение с использованием короткого имени компьютера» может быть установлен в случае, когда сервер EndpointSniffer находится в другом домене или в рабочей группе, и подключение по полному имени невозможно.

По умолчанию агенты EndpointSniffer работают под системной учетной записью. При необходимости учетная запись выбранной рабочей станции с установленным агентом может быть изменена (например, при нехватке прав у текущей учетной записи на работу с агентом на рабочей станции, находящейся в другом домене). Настройка учетной записи производится на вкладке «Запускать от имени».

На вкладке «Передача данных» вкладки «Настройки» можно разрешить/запретить запуск агентов при загрузке операционной системы в безопасном режиме. Установленный флажок разрешает запуск агентов в безопасном режиме, снятый – запрещает. С помощью параметра «Число попыток передачи данных на сервер» можно задать количество попыток передачи сообщения агентом на сервер. Если все попытки окажутся неудачными, агент будет пробовать передать сообщение на другие серверы из списка имеющихся серверов. Если ни один из серверов не ответит, агент будет переключен в режим оффлайн. Значения остальных параметров, установленные по умолчанию, могут быть изменены для каждого компьютера.

Флажок в строке «Включить передачу данных с агентов по расписанию». Данная настройка может использоваться для уменьшения нагрузки на сеть при малом пропускном канале. По умолчанию передача данных осуществляется постоянно, сразу после установки. Можно задать временной промежуток

Библиотека БГУИР

(начало, окончание, дни недели), в течение которого агент будет передавать данные на сервер. На рис. 2.51 представлен пример выполнения настроек на вкладке «Передача данных».

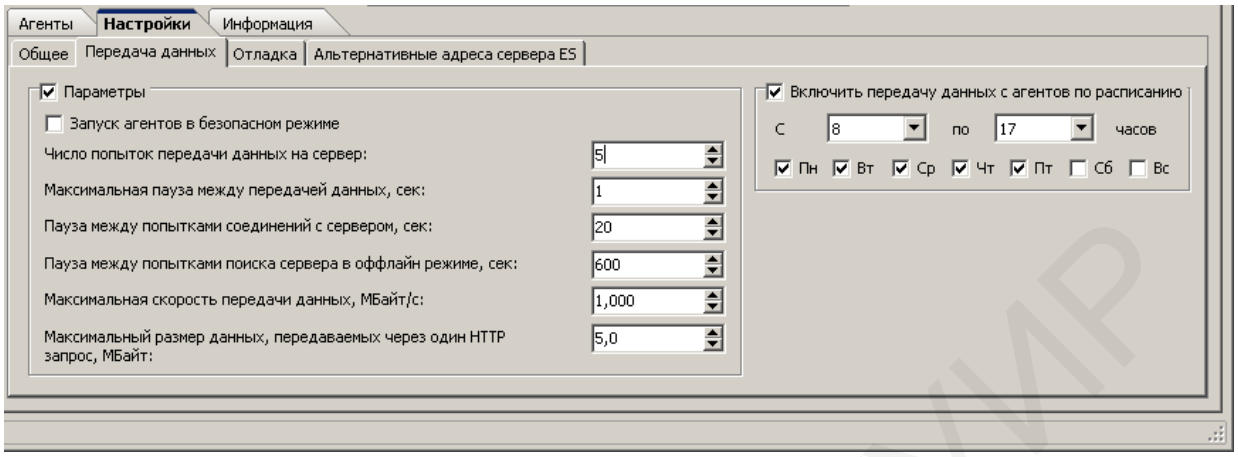


Рис. 2.51. Вкладка «Передача данных»

Настройки управления логированием агентов для выбранной рабочей станции производятся на вкладке «Отладка» (рис. 2.52). Доступны следующие значения:

– «Выключено» – логирование не осуществляется;

– «Нормальное» – логируются только важные события;

– «Подробно» – логируются все операции.

Для сохранения лог-файлов используется кнопка «Получить логи».

Сохраненные логи размещаются по умолчанию в папке: %Program Files%\SearchInform\SearchInform EndpointSniffer\service\

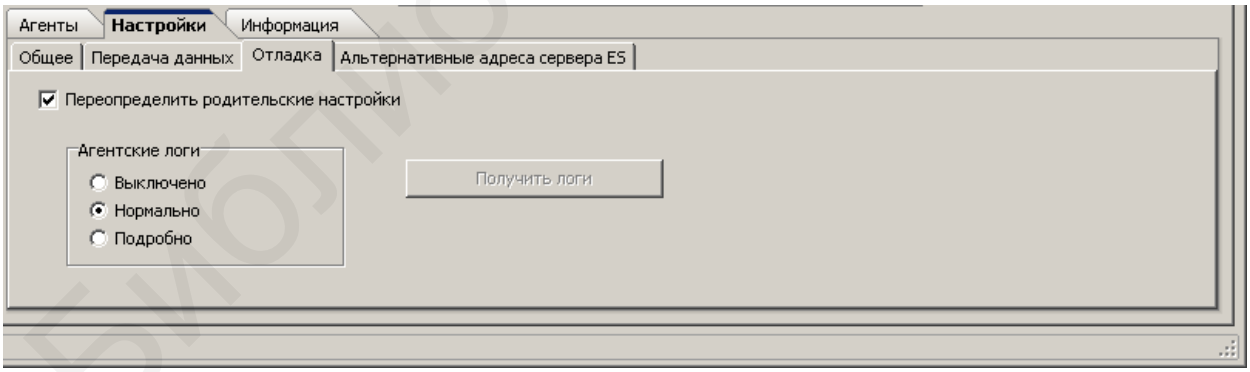


Рис. 2.52. Настройки управления логированием агентов

Вкладка «Альтернативные адреса сервера ES» используется для добавления адресов сервера ES, к которым будет обращаться агент в случае отсутствия доступа к основному серверу. Для добавления, редактирования или удаления альтернативного адреса используются соответственно кнопки «Добавить», «Редактировать» и «Удалить» (рис. 2.53).

Библиотека БГУИР

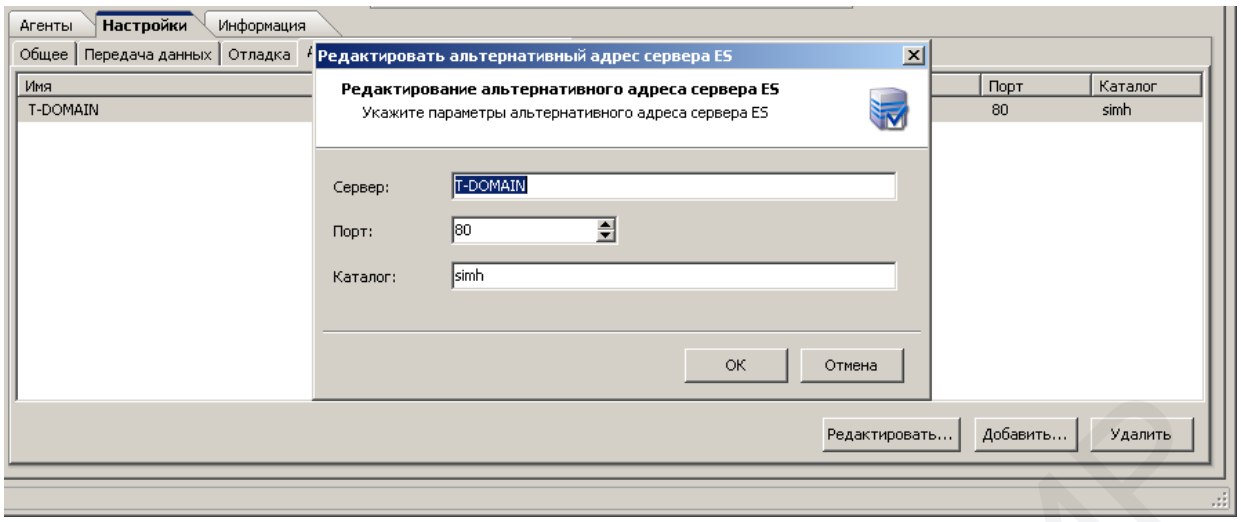


Рис. 2.53. Ввод адресов, к которым обращается агент
в случае отсутствия доступа к серверу

На вкладке «Заметки» вкладки «Информация» отображается сводка состояния выделенного компьютера (рис. 2.54). По результатам генерации кода (глобального кода) для остановки агентов на вкладке «Заметки» отображается сгенерированный код (глобальный код).

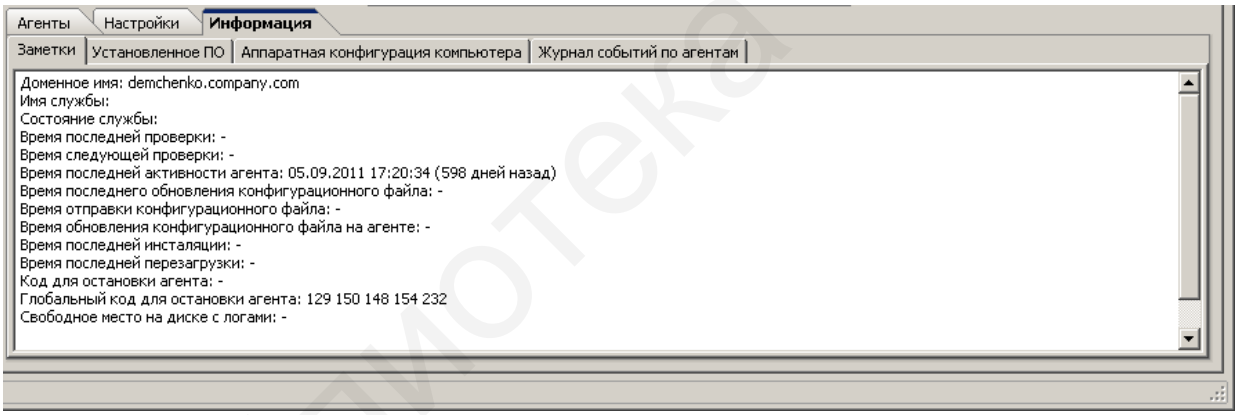


Рис. 2.54. Сводка состояния выделенного компьютера

На вкладке «Установленное ПО» отображаются маркеры программного обеспечения, установленного на выбранной рабочей станции (рис. 2.55).

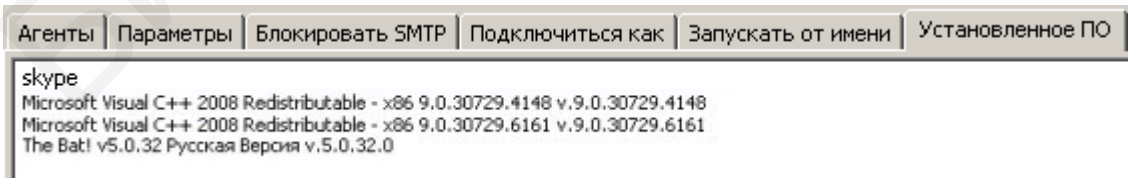


Рис. 2.55. Маркеры программного обеспечения,
установленного на выбранной рабочей станции

На вкладке «Аппаратная конфигурация компьютера» отображаются данные об аппаратной конфигурации рабочей станции (рис. 2.56).

Библиотека БГУИР

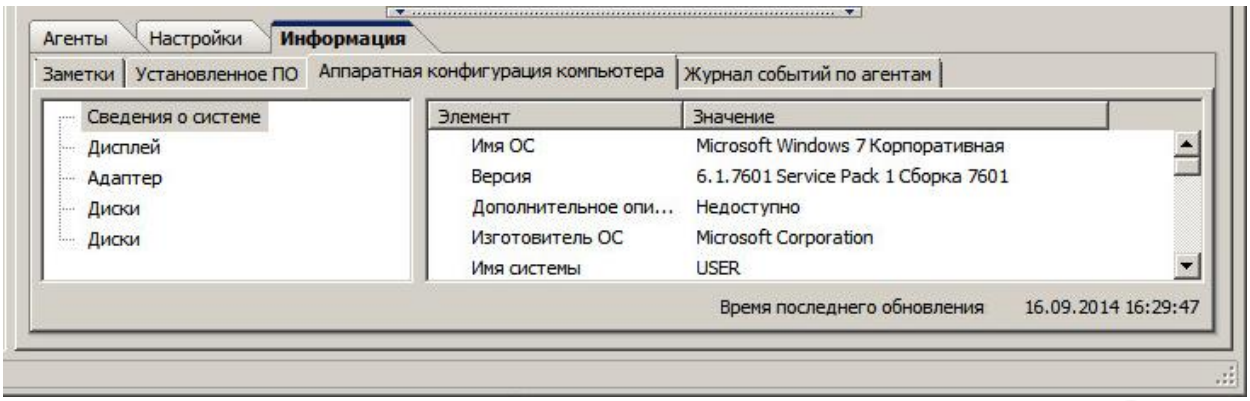


Рис. 2.56. Аппаратная конфигурация компьютера

На вкладке «Журнал событий по агентам» отображаются сведения о проблемах в работе агентов.

Поддерживаемые платформы. Работа агентов поддерживается в следующих операционных системах семейства Windows:

– Server 2003, x32/x64;
– XP, x32/x64;
– Vista, x32/x64;
– Server 2008 x32/x64;
– Server 2008 R2 x64;
– Windows 7, x32/x64.

2.4.1. Агент DeviceSniffer

Агент DeviceSniffer предназначен для управления доступом к внешним устройствам и буферу обмена, а также для перехвата данных, передаваемых на подключаемые внешние устройства и управления доступом к процессам, выполняемым на рабочих станциях.

Управление агентом производится на вкладке «Агенты» консоли администрирования. Для доступа к настройкам следует выделить протокол Device и вызвать окно редактирования настроек агента любым из нижеперечисленных способов (рис. 2.57):

– двойным щелчком кнопки мыши по названию протокола;
– нажатием кнопки  в верхней части консоли;
– нажатием кнопки «Дополнительно...».

В окне редактирования агента DeviceSniffer можно выполнять следующие задачи:

– производить настройки агента DeviceSniffer и внешних устройств;
– добавлять внешние устройства в «белый список»;
– обращаться к журналу аудита и теневого копирования данных, записываемых на внешнее устройство.

Библиотека БГУИР

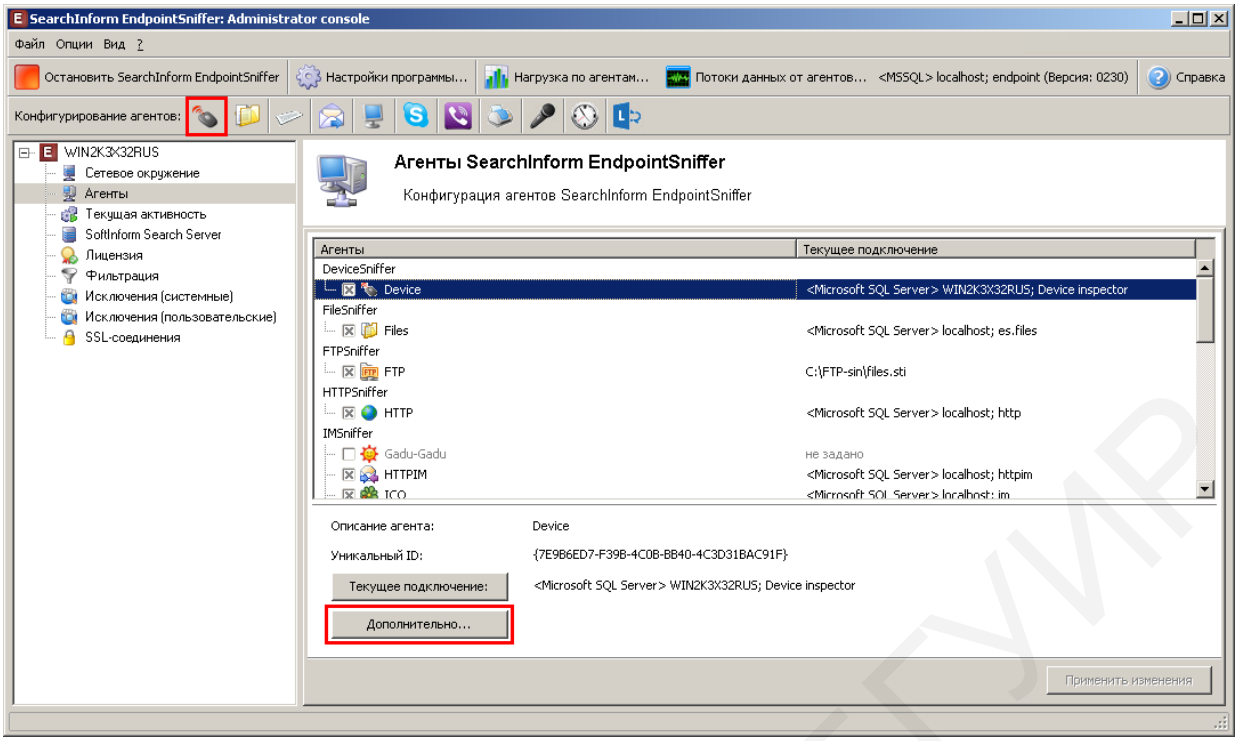


Рис. 2.57. Управление агентом DeviceSniffer

Настройка агента DeviceSniffer выполняется на вкладке «Настройки» окна редактирования агента DeviceSniffer. Указанная вкладка отображает список внешних устройств, передача данных на которые может ограничиваться либо контролироваться агентом (рис. 2.58).

Список окна редактирования агента DeviceSniffer включает следующие элементы:

– «ИК-порт» – устройства, использующие в качестве среды передачи данных инфракрасный диапазон световых волн;

– «Медиа» – аудио- и видеоустройства, игровые манипуляторы, другие мультимедийные устройства;

– «HID-устройство» – устройства-манипуляторы (human interface device): клавиатура, мышь, игровой контроллер и т. д.;

– «FireWire» – устройства, подключаемые к компьютеру при помощи шины IEEE 1394 (как правило, бытовые и профессиональные электронные приборы, относящиеся к категории записывающей и воспроизводящей видео- и аудиоаппаратуры);

– «Сетевая папка» – все сетевые папки;

– «Смарт-карта» – устройства USB со встроенной микросхемой;

– «КПК» – портативные вычислительные устройства, обладающие широкими функциональными возможностями;

– «Ленточный накопитель» – запоминающие устройства, работа которых основана на принципе магнитной записи на ленточный носитель и которые характеризуются последовательным доступом к данным и предназначены для записи/воспроизведения информации, архивации и резервного копирования данных;

– «Процессы» – блокировка и мониторинг запуска определенных процессов;

Библиотека БГУИР

– «Буфер обмена» – блокировка и мониторинг копирования данных в буфер обмена;

– «Переносные устройства Windows» – устройства со встроенным драйвером, поддерживающие широкий спектр портативных устройств (мобильные телефоны, цифровые камеры, медиаплейеры и т. п.).

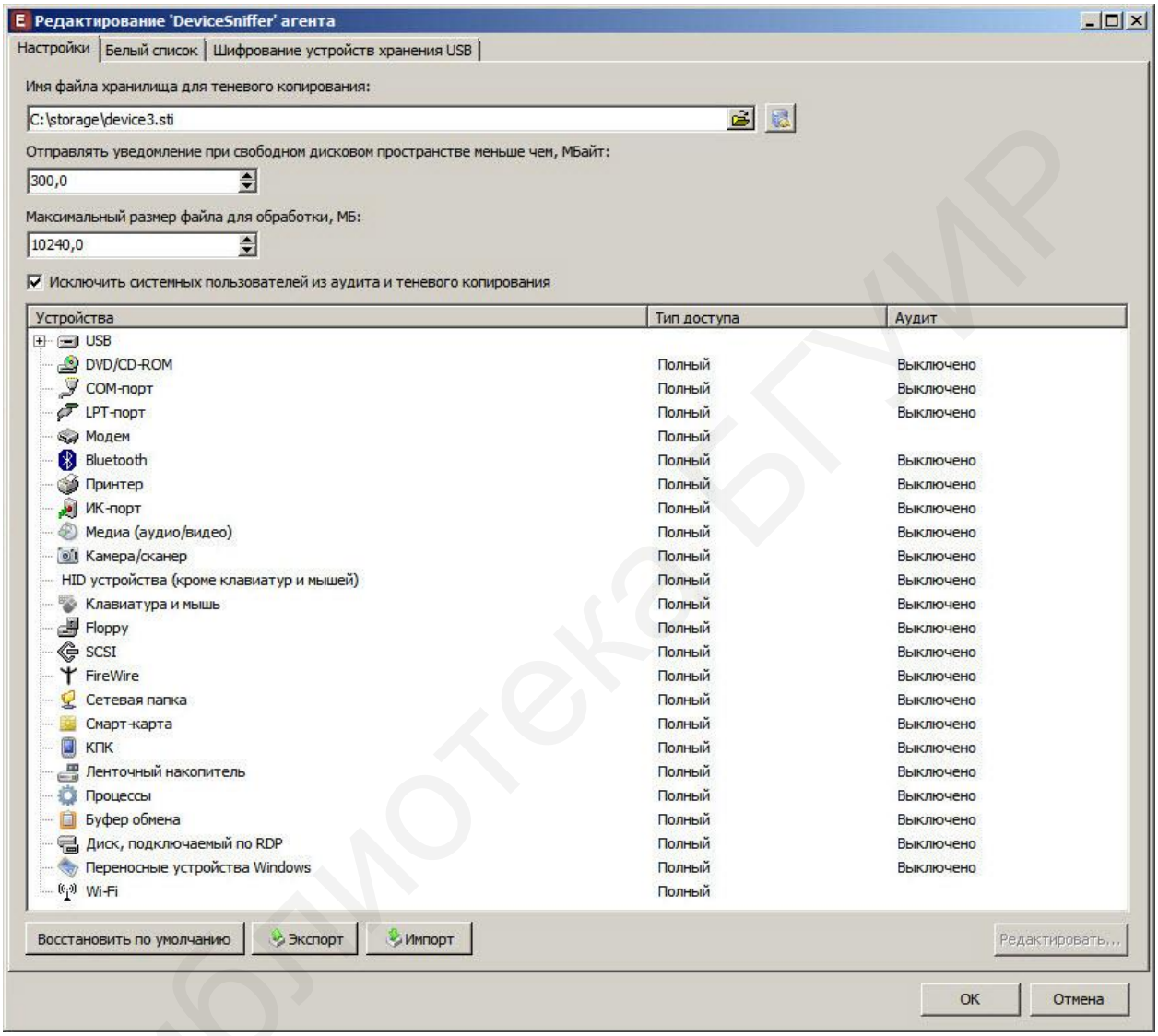


Рис. 2.58. Настройка агента DeviceSniffer

Устройства, подключаемые при помощи USB, образуют отдельный узел – USB, причем настройка каждого из них производится автономно, в то время как в совокупности они редактироваться не могут (кнопка «Редактировать» при выделении узла USB становится неактивной). Опция «Все устройства USB (кроме концентраторов USB)» предназначена для управления доступом ко всем устройствам USB за исключением концентраторов.

Над списком расположена строка для указания пути к sti-файлу хранилища, в которое помещаются данные в результате теневого копирования, а также регулятор, предназначенный для ограничения размера файла, к которому будет

Библиотека БГУИР

применено теневое копирование. Значение максимального размера файла вводится вручную либо выбирается стрелками регулятора.

При установленном флажке (над списком внешних устройств) системные пользователи исключаются из аудита и теневого копирования. В качестве системных пользователей выступают учетные записи, от имени которых выполняются системные службы (их работа, как правило, не представляет интереса для аудиторов безопасности).

Расположенная под списком внешних устройств кнопка «Восстановить по умолчанию» служит для сброса всех пользовательских настроек агента DeviceSniffer.

Настроенная конфигурация параметров агента DeviceSniffer может быть экспортирована в указанный пользователем файл формата XML. В свою очередь, сохраненная конфигурация настроек может быть импортирована в приложение из указанного пользователем файла. Для экспорта/импорта конфигурации используются кнопки «Экспорт» и «Импорт».

Настройки доступа к внешним устройствам производятся с помощью кнопки «Редактировать» в правом нижнем углу окна редактирования агента DeviceSniffer. При этом становится возможным решать следующие задачи:

– управление доступом к внешнему устройству;

– управление аудитом операций, выполняемых внешним устройством;

– управление доступом для пользователей (групп), которые работают с внешними устройствами;

– управление доступом для компьютеров, на которых используются внешние устройства;

– теневое копирование данных, передаваемых на внешнее устройство;

– выборочное теневое копирование по типам файлов;

– управление доступом к процессам;

– управление доступом к буферу обмена.

Все настройки доступа и аудита производятся через окно редактирования выбранного внешнего устройства (рис. 2.59). Расположенная в нем кнопка «Восстановить по умолчанию» отменяет все произведенные настройки и приводит конфигурацию для выбранного устройства в исходное состояние.

Для управления доступом к внешнему устройству используется выпадающий список «Тип доступа». Всего предусмотрено три типа доступа к внешнему устройству:

– «Запретить доступ» – для полной блокировки внешнего устройства;

– «Полный» – для открытия доступа к внешнему устройству;

– «Только чтение» – для предоставления ограниченного доступа, когда использование внешнего устройства позволяет пользователю работать с данными в режиме «только чтение» (данная опция предусмотрена не для всех внешних устройств).

Для выбора операций, которые будут отслеживаться и протоколироваться агентами DeviceSniffer, используется выпадающий список «Аудит».

Библиотека БГУИР

Опции «Выключено» и «Полный» предусмотрены для всех типов внешних устройств, присутствие остальных опций зависит от типа устройства.

Предусмотрены следующие типы аудита внешнего устройства:

– «Выключено» – для выключения аудита; при этом совершаемые операции при использовании выбранного внешнего устройства фиксироваться не будут;

– «Полный» – для включения аудита и протоколирования операций, выполняемых внешним устройством;

– «Чтение» – для отслеживания операций по просмотру (чтению) данных;

– «Запись» – для отслеживания операций по записи данных;

– «Другое» – для отслеживания других операций с использованием внешнего устройства, таких как открытие, подключение, чтение, запись, удаление, переименование, выполнение, форматирование.

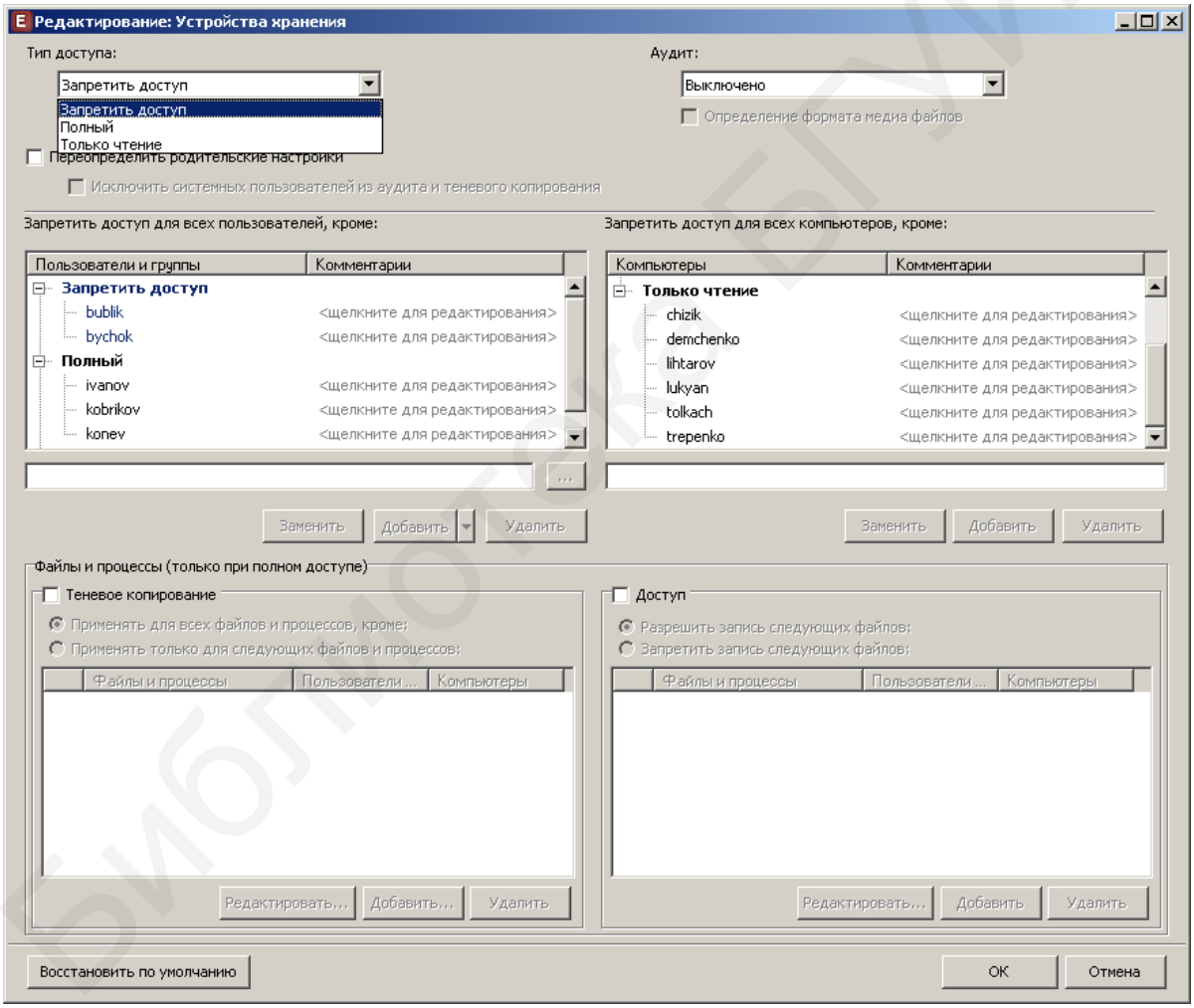


Рис. 2.59. Настройка доступа и аудита внешнего устройства

Разрешение и ограничение доступа к внешнему устройству может быть применено к отдельным пользователям и группам. Для этого в колонке «Пользователи и группы» необходимо выбрать тип доступа. В табл. 2.2 представлены возможные варианты доступа в отношении отдельных пользователей (групп), исходя из текущего типа доступа к внешнему устройству.

Библиотека БГУИР

Следует помнить, что приоритет отдельного пользователя выше приоритета отдельного компьютера. Проиллюстрируем это следующим примером. Предположим, что для всех пользователей установлено правило «запретить доступ», в то время как для пользователя user1 – «полный доступ», для компьютера computer1 – «только чтение». В этом случае user1 получит полный доступ к внешнему устройству на всех компьютерах, пользователи computer1 (за исключением user1) будут иметь доступ с правом «только чтение». При этом для всех остальных компьютеров и пользователей доступ к внешнему устройству будет запрещен.

Таблица 2.2

Возможные варианты доступа в отношении отдельных пользователей (групп)/компьютеров

Тип доступа к внешнему устройству	**Тип доступа по отношению к пользователям/компьютерам**
Доступ запрещен	Разрешить полный доступ. Разрешить доступ только для чтения
Доступ разрешен	Запретить доступ. Разрешить доступ только для чтения
Доступ частично ограничен (только чтение)	Разрешить полный доступ. Запретить доступ

Далее необходимо ввести имя пользователя (группы) в текстовое поле.

Ввод имени группы осуществляется в формате DOMAIN\group; ввод имени пользователя – в формате user@domain.local.

На добавленного пользователя (группу) будет распространен выбранный тип доступа к устройству. К отдельным пользователям (группам) можно добавить также все доменные (пункт «Любой доменный пользователь») либо все локальные (пункт «Любой локальный пользователь») учетные записи с помощью выпадающего меню.

Для импорта пользователя (группы) нужно воспользоваться кнопкой  . В открывшемся окне (рис. 2.60) следует выбрать способ получения списка пользователей (из DataCenter, Active Directory либо NetBIOS), при помощи флажков – группы или пользователей в домене, после чего нажать кнопку «Добавить».

Если список пользователей достигает больших размеров, можно воспользоваться поиском/фильтрацией. Для этого необходимо ввести запрос в строку «Поиск» и при помощи кнопки «Начинающийся с …» или «Содержащий …» определить, в какой части значения атрибута искать введенное значение.

Разрешение и ограничение доступа к внешнему устройству может быть применено и к отдельным компьютерам. Для этого в колонке «Компьютеры» необходимо выбрать тип доступа. В табл. 2.2 представлены возможные варианты доступа в отношении отдельных компьютеров, исходя из текущего типа доступа к внешнему устройству.

Библиотека ВГАВМ

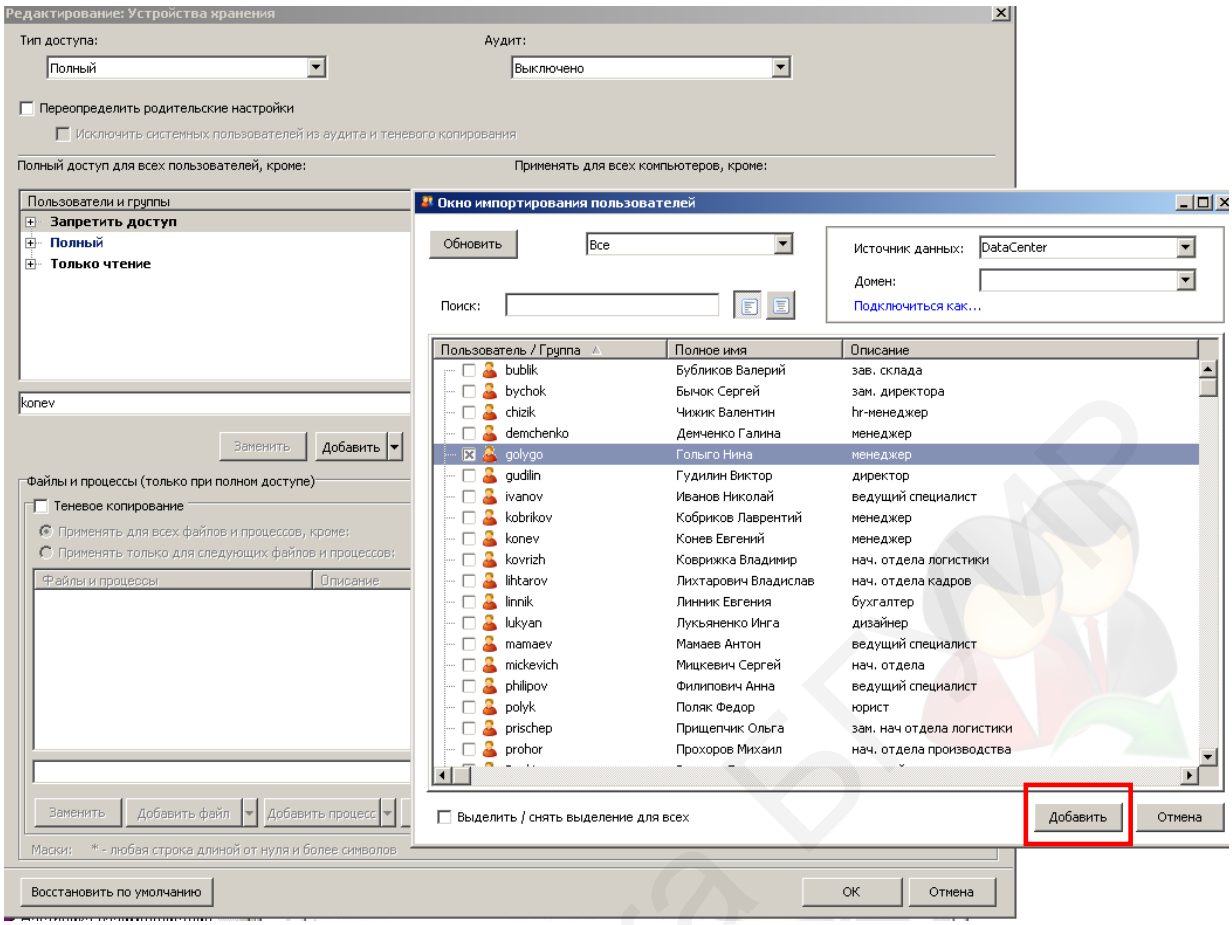


Рис. 2.60. Настройка доступа и аудита внешнего устройства для отдельного пользователя

Для выбора компьютера, на который будет распространяться соответствующий тип доступа, необходимо воспользоваться кнопкой «Добавить» (ввод имени компьютера вручную не предусмотрен). В открывшемся окне «Выбор компьютеров» путем установки/снятия флажков необходимо указать компьютеры/группы, на которых доступ к внешнему устройству будет разрешен либо ограничен (рис. 2.61). Если список компьютеров достигает больших размеров, можно воспользоваться поиском/фильтрацией аналогично тому, как это было рассмотрено применительно к настройке доступа для отдельных пользователей.

После нажатия кнопки «ОК» выбранные компьютеры будут добавлены в список. Система предупредит о компьютерах, имена которых уже находились в списке.

Для замены одного компьютера другим либо удаления компьютера из зоны действия настраиваемого типа доступа необходимо воспользоваться кнопками «Заменить»/«Удалить».

Для включения режима теневого копирования данных следует установить флажок в строке «Теневое копирование» (рис. 2.62). Теневое копирование работает только на устройствах, к которым открыт полный доступ. Помимо настроек непосредственно самого устройства, полный доступ может быть открыт посредством включения его в так называемый «белый список».

Библиотека БГУИР

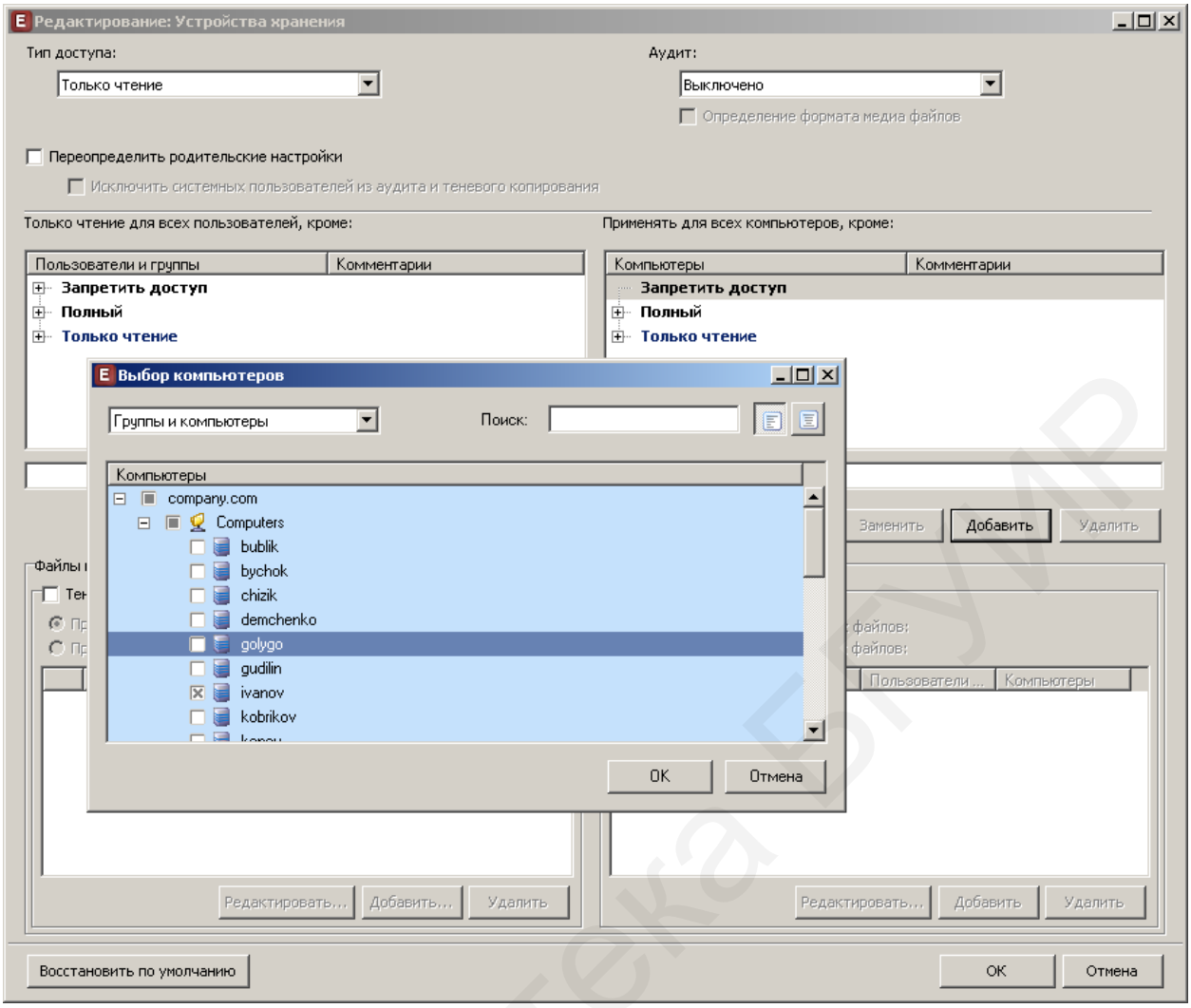


Рис. 2.61. Настройка доступа и аудита внешнего устройства для отдельного компьютера

Теневое копирование может быть применено к отдельным пользователям (группам пользователей), компьютерам, форматам файлов и процессам. Для обеспечения удобства использования данной функции можно выбрать соответствующую опцию (при наличии флажка в чекбоксе «Теневое копирование»):

– «Применять для всех файлов и процессов, кроме…» – копирование будет применяться ко всем файлам и процессам, за исключением указанных;

– «Применять только для следующих файлов и процессов…» – копирование будет применяться только к указанным файлам и процессам.

Теневое копирование взаимосвязано с доступом к файлам. Например, если доступ разрешен только к определенным файлам, то и применить операцию теневого копирования можно будет только к этим файлам. Нельзя применить теневое копирование к файлам, доступ к которым запрещен.

Библиотека БГУИР

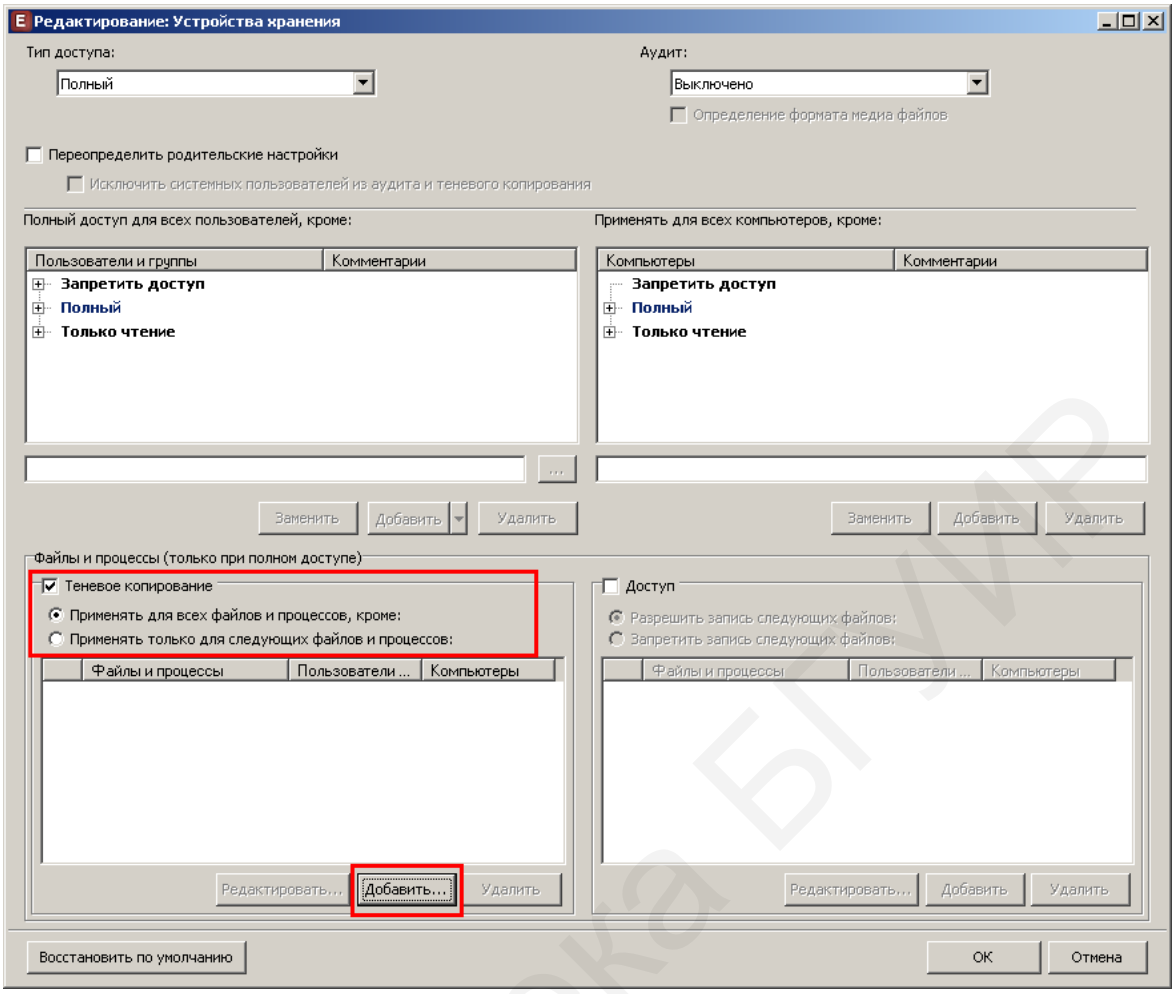


Рис. 2.62. Включение режима теневого копирования данных

DeviceSniffer позволяет настраивать правила теневого копирования для отдельных пользователей (групп), а также отдельных компьютеров. Таким образом, можно настроить, например, теневое копирование для файла *.doc только для пользователя user1 и/или компьютера computer2.

Для добавления правил теневого копирования нажмите «Добавить» (рис. 2.63).

Введите в текстовое поле имя файла или процесса и нажмите кнопку:

– «Добавить файл» – для добавления файла в список, на который распространяется выбранное правило;

– «Добавить процесс» – для добавления процесса в список, на который распространяется выбранное правило.

Чтобы указать, какой именно файл либо процесс подлежит теневому копированию, следует ввести в текстовое поле имя файла или процесса (рис. 2.64). Расположенная справа от текстового поля кнопка позволяет выбрать переменные среды пользователя.

DeviceSniffer позволяет применять правила не только к отдельным файлам, но и к типам файлов. Настройка производится в окне со списком типов файлов. Для того чтобы получить доступ к указанному информационному окну,

Библиотека БГУИР

нужно щелкнуть по стрелке рядом с кнопкой «Добавить файл» и выбрать одну из двух опций:

– «По имени...» – для применения правила к типам файлов в случае, если тип файла определяется расширением, указанным в имени файла;

– «По типу...» – для применения правила к типам файлов в случае, если тип файла определяется выполняемым процессом.

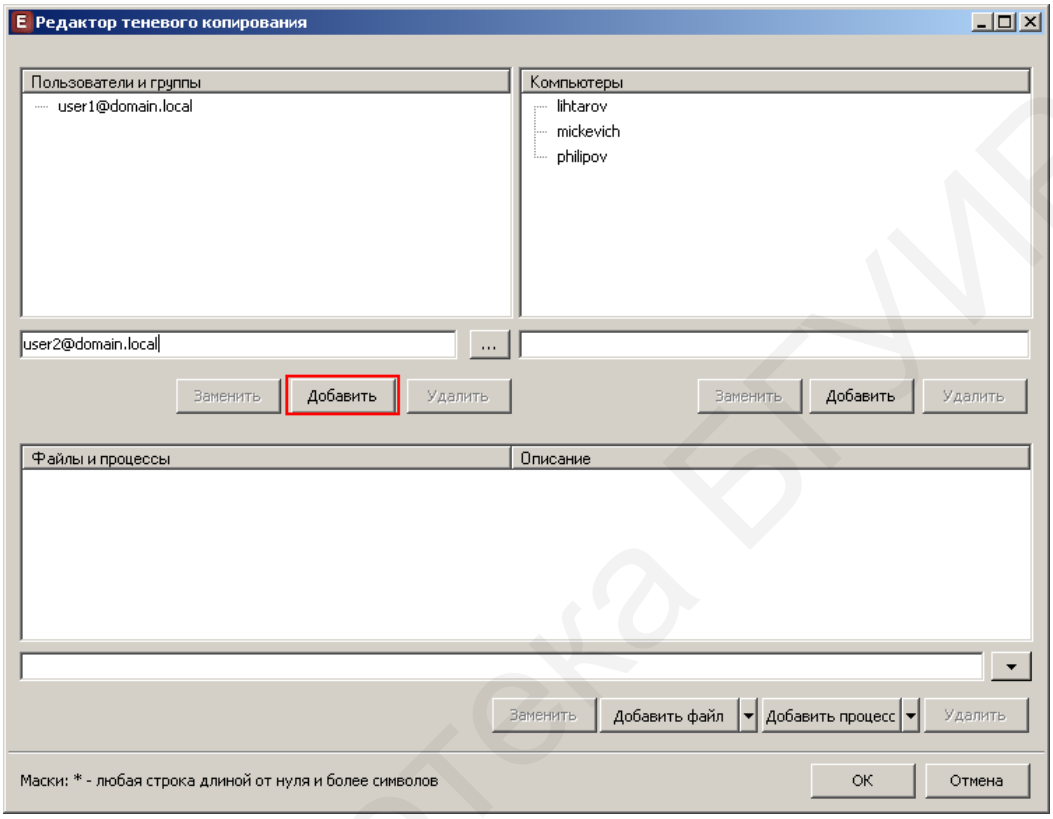


Рис. 2.63. Редактор правил теневого копирования

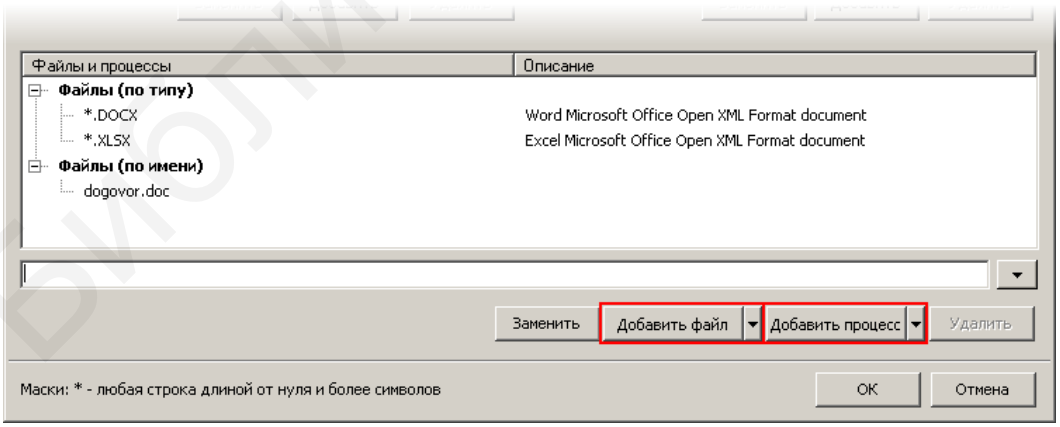


Рис. 2.64. Добавление файлов/процессов в список, на который будет распространяться выбранное правило теневого копирования данных

Библиотека БГУИР

В открывшемся окне «Типы файлов» (рис. 2.65) устанавливаются флажки напротив тех типов файлов, к которым должно быть применено выбранное правило.

После нажатия кнопки «OK» выбранные типы файлов будут добавлены в зону действия правила.

Для замены файла (типа файла, процесса) другим либо удаления его из зоны действия выбранного правила необходимо воспользоваться кнопками «Заменить»/«Удалить».

Для сохранения произведенных настроек следует нажать «OK» в окне редактирования настроек выбранного внешнего устройства.

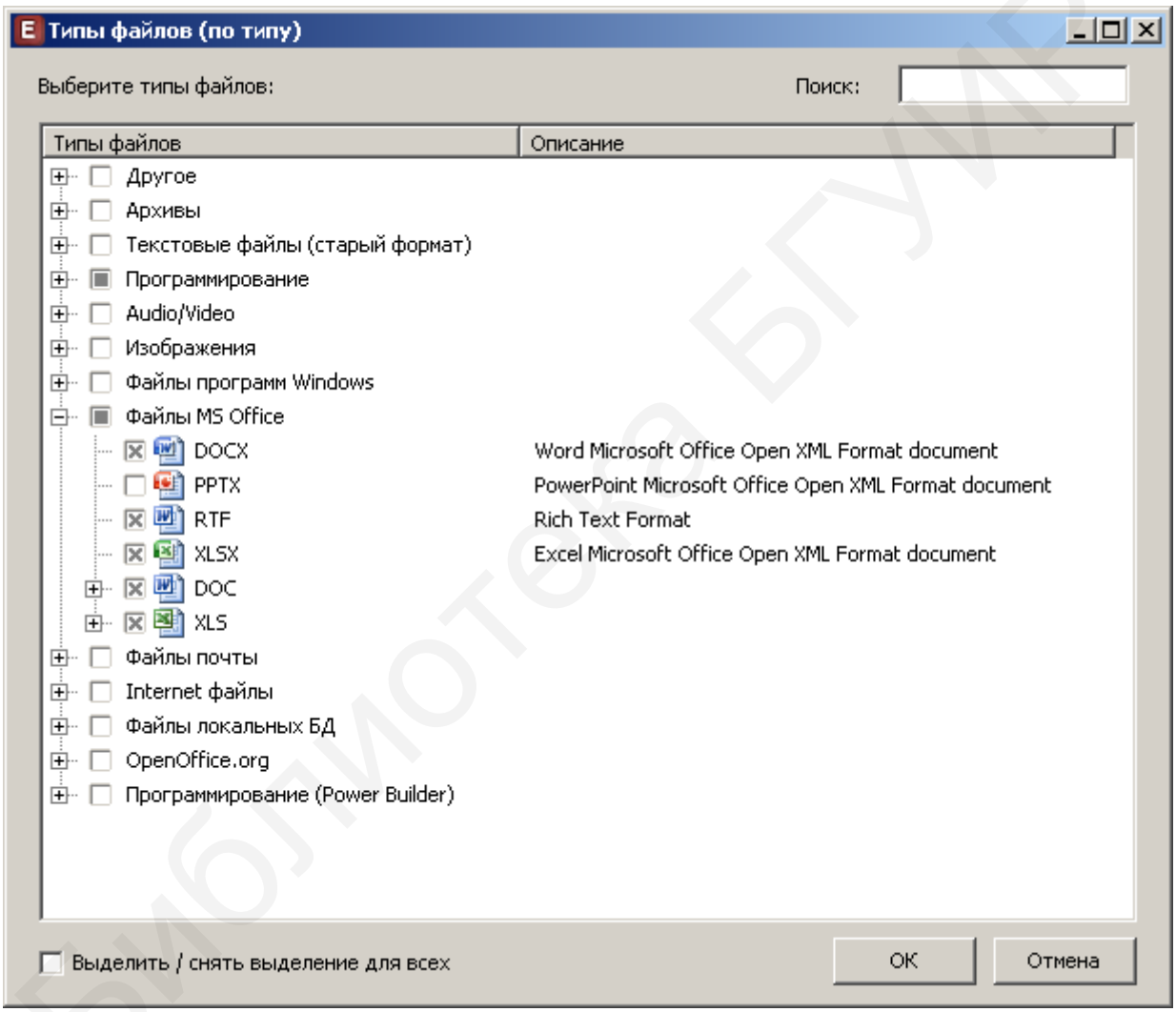


Рис. 2.65. Окно «Типы файлов»

Управление доступом к файлам. Для включения правил доступа к файлам, записываемым на внешние устройства, нужно установить флажок в строке «Доступ» (рис. 2.66). После этого становится доступным выбор одного из двух правил:

– «Разрешить запись следующих файлов»;

– «Запретить запись следующих файлов».

Библиотека БГУИР

Как уже говорилось ранее, доступ к файлам взаимосвязан с теневым копированием. Если доступ разрешен только к определенным файлам, то и применить операцию теневого копирования можно будет только к этим файлам. Нельзя применить теневое копирование к файлам, доступ к которым запрещен.

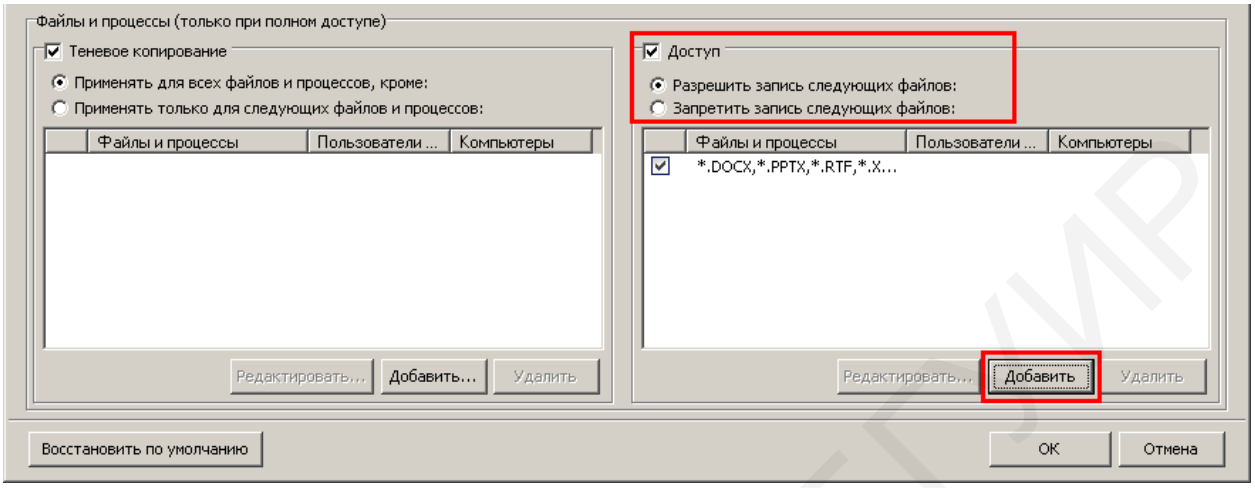


Рис. 2.66. Добавление файлов/процессов в список, на который будет распространяться выбранное правило теневого копирования данных

DeviceSniffer позволяет настраивать правила доступа для отдельных пользователей (групп), а также отдельных компьютеров. Таким образом, можно настроить, например, доступ к файлу *.doc только для пользователя user1 и/или компьютера computer2.

Кроме того, настройку можно производить и по типам файлов. Для этого необходимо щелкнуть по стрелке рядом с кнопкой «Добавить файл» и выбрать одну из двух опций:

– «По имени...» – для применения правила к типам файлов в случае, если тип файла определяется расширением, указанным в имени файла;

– «По типу...» – для применения правила к типам файлов в случае, если тип файла определяется выполняемым процессом.

Управление доступом к процессам применяется только для одной позиции в списке внешних устройств – «Процессы» (рис. 2.67), предназначенной для блокировки и мониторинга запуска определенных процессов. Для осуществления соответствующей настройки следует выделить указанную позицию и нажать кнопку «Редактировать» окна редактирования агента DeviceSniffer.

Имеющиеся настройки в окне редактирования процессов позволяют выбрать пользователей и компьютеры, к которым будут применены блокировка доступа к процессам и аудит соответствующих операций, а также непосредственно сами процессы, которые будут подвергнуты блокировке.

Библиотека БГУИР

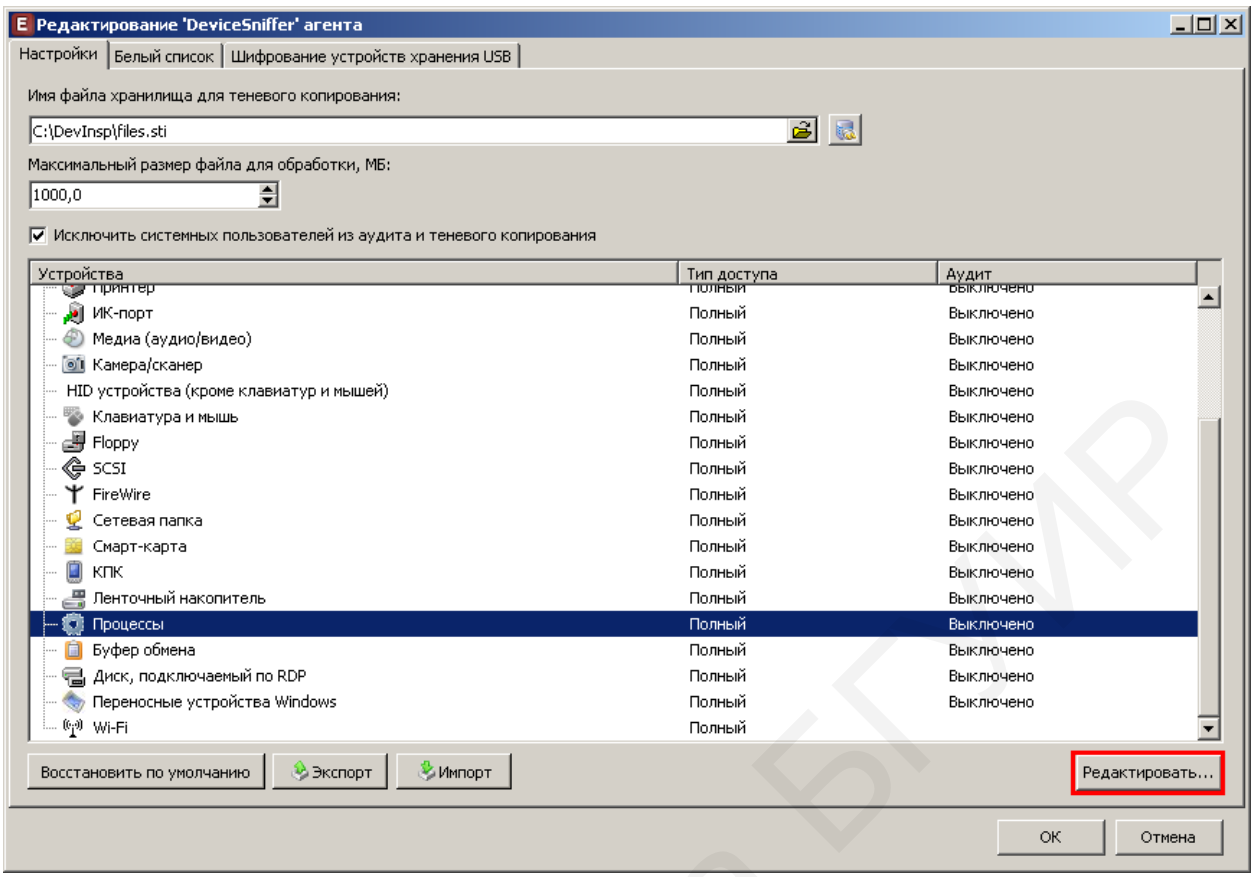


Рис. 2.67. Настройка управления доступом к процессам

Нужно помнить, что агент DeviceSniffer исключает возможность блокировки всех процессов. Нажатие кнопки «ОК» при установленном флажке и отсутствие каких-либо других настроек вызовет предупреждение о необходимости выбрать фильтр процессов.

Выбор пользователей и компьютеров, к которым будет применена блокировка доступа к процессам, осуществляется аналогично тому, как это было рассмотрено для управления доступом к внешнему устройству.

Для добавления правил нажмите «Добавить» (рис. 2.68).

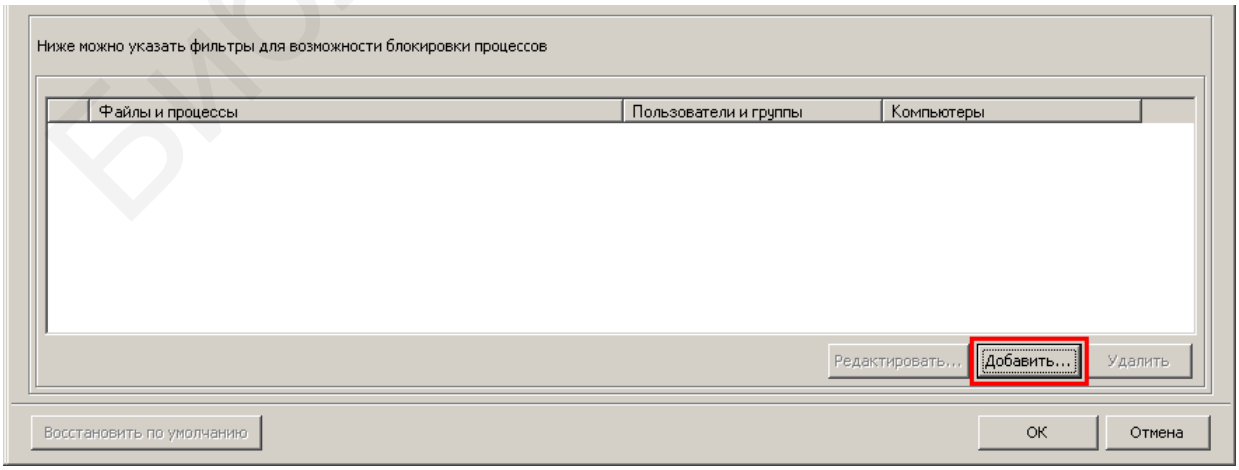


Рис. 2.68. Добавление правил доступа к процессам

Библиотека БГУИР

В открывшемся окне редактора процессов настройте правила блокировки. Выбор пользователей (групп) и компьютеров осуществляется так же, как и при теневом копировании. Для выбора процессов, которые будут подвергнуты блокировке, используются элементы управления в нижней части окна редактирования процессов. Для того чтобы осуществить блокировку, следует ввести в текстовое поле имя файла или процесса и нажать одну из следующих кнопок (рис. 2.69):

– «Добавить родительский процесс» – блокировка всех дочерних процессов, порожденных указанным процессом;

– «Добавить процесс» – блокировка только указанного процесса.

Символ маски (*) означает, что в качестве значения параметра может выступать строка любой длины. Расположенная справа от текстового поля кнопка позволяет выбрать переменные среды пользователя.

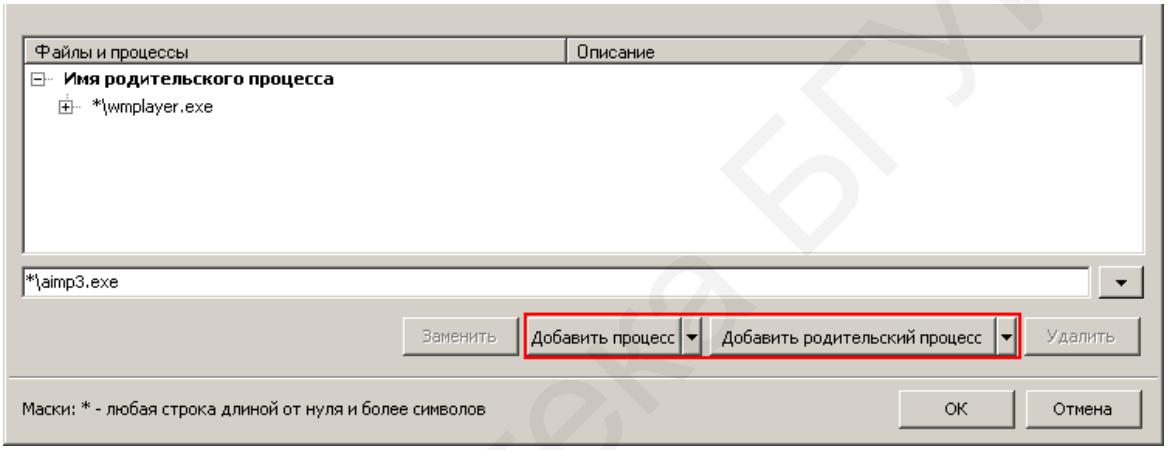


Рис. 2.69. Добавление процессов, которые будут подвергнуты блокировке

Для включения аудита всех операций, связанных с блокированием процессов, необходимо выбрать опцию «Полный» в раскрывающемся списке «Аудит» (рис. 2.70), для сохранения всех произведенных настроек по управлению доступом к процессам – нажать кнопку «OK» в окне редактирования процессов.

Управление доступом к буферу обмена также применяется только для одной позиции в списке внешних устройств – «Буфер обмена», предназначенной для блокировки и мониторинга копирования данных в буфер обмена (рис. 2.71).

Для осуществления соответствующей настройки следует выделить указанную позицию и нажать кнопку «Редактировать» окна редактирования агента DeviceSniffer.

Имеющиеся настройки в окне редактирования позволяют выбрать пользователей и компьютеры, к которым будет применена блокировка доступа к буферу обмена, а также фильтры для возможности блокировки буфера обмена по полному пути к родительскому процессу.

Нажатие кнопки «OK» при выбранной опции «Запретить доступ» и отсутствии каких-либо других настроек закрывает доступ к буферу обмена

для всех компьютеров сети, на которых установлен и включен агент DeviceSniffer.

Выбор пользователей и компьютеров, к которым будет применена блокировка доступа к процессам, осуществляется аналогично тому, как это было рассмотрено для управления доступом к внешнему устройству или процессам.

Для возможности блокировки буфера обмена по полному пути к родительскому процессу используются элементы управления в нижней части окна редактирования процессов. Для добавления фильтра следует ввести в текстовое поле имя процесса и нажать кнопку «Добавить процесс» (рис. 2.72). Расположенная справа от текстового поля кнопка  позволяет выбрать переменные среды пользователя.

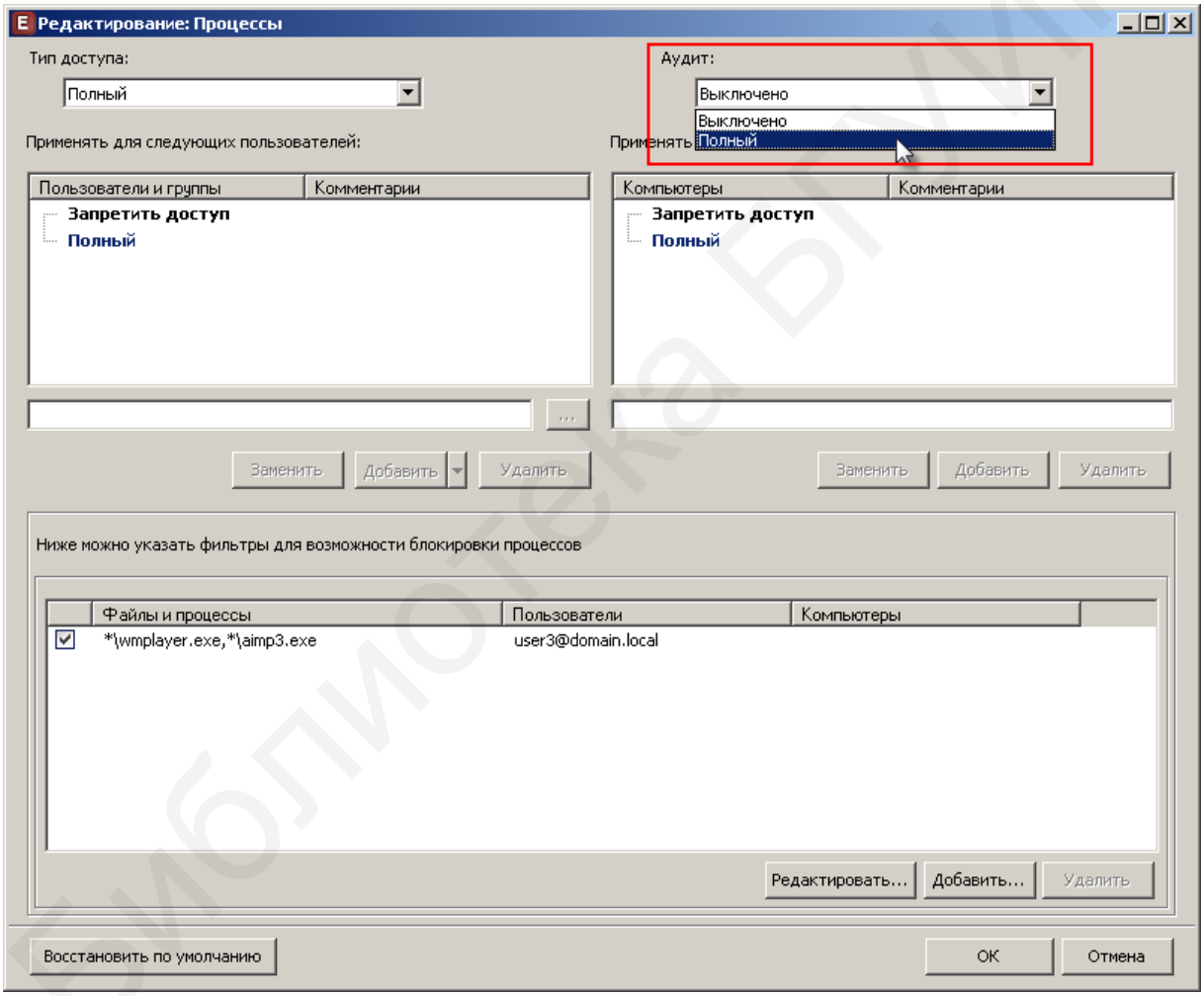


Рис. 2.70. Включение аудита всех операций, связанных с блокированием процессов

Для включения аудита всех операций, связанных с блокированием доступа к буферу обмена, необходимо выбрать опцию «Полный» в раскрывающемся списке «Аудит», для сохранения всех произведенных настроек по управлению доступом к буферу обмена – нажать кнопку «OK» в окне редактирования.

Библиотека БГУИР

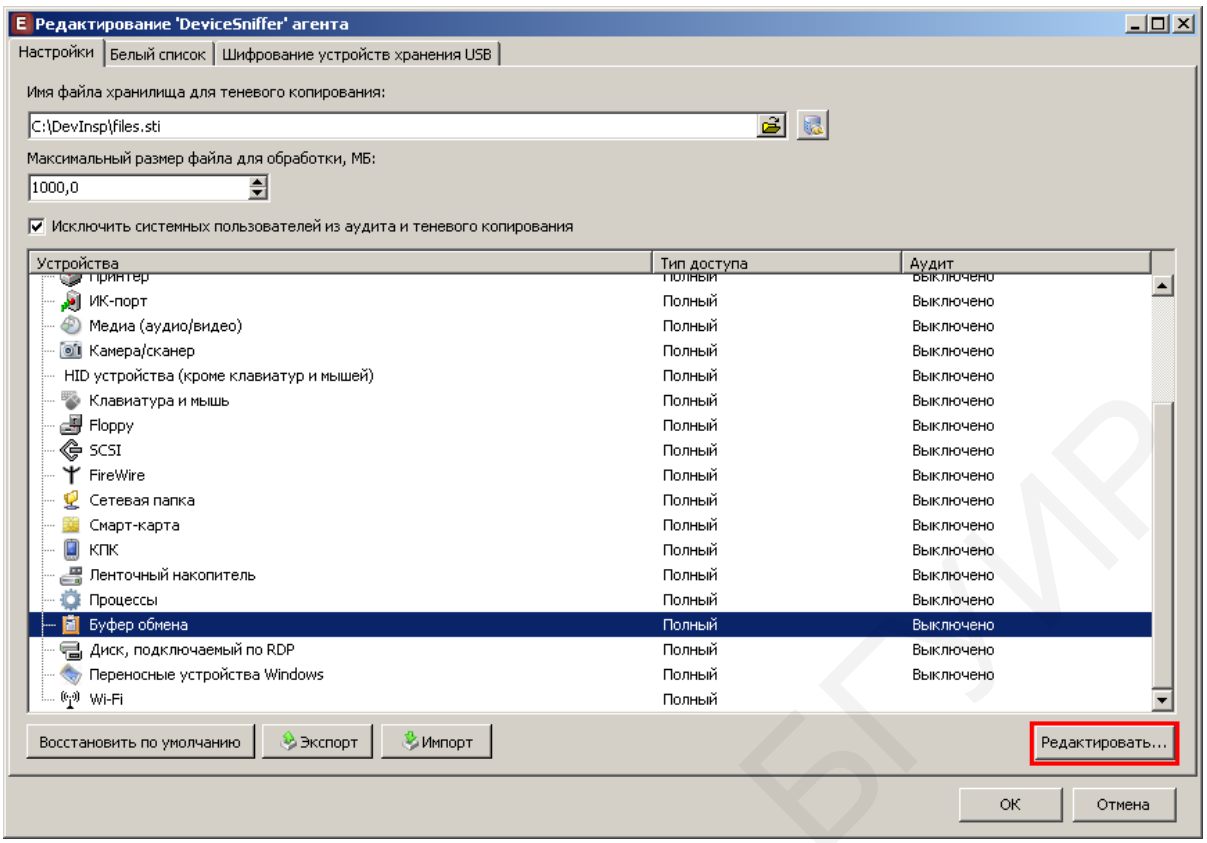


Рис. 2.71. Настройка управления доступом к буферу обмена

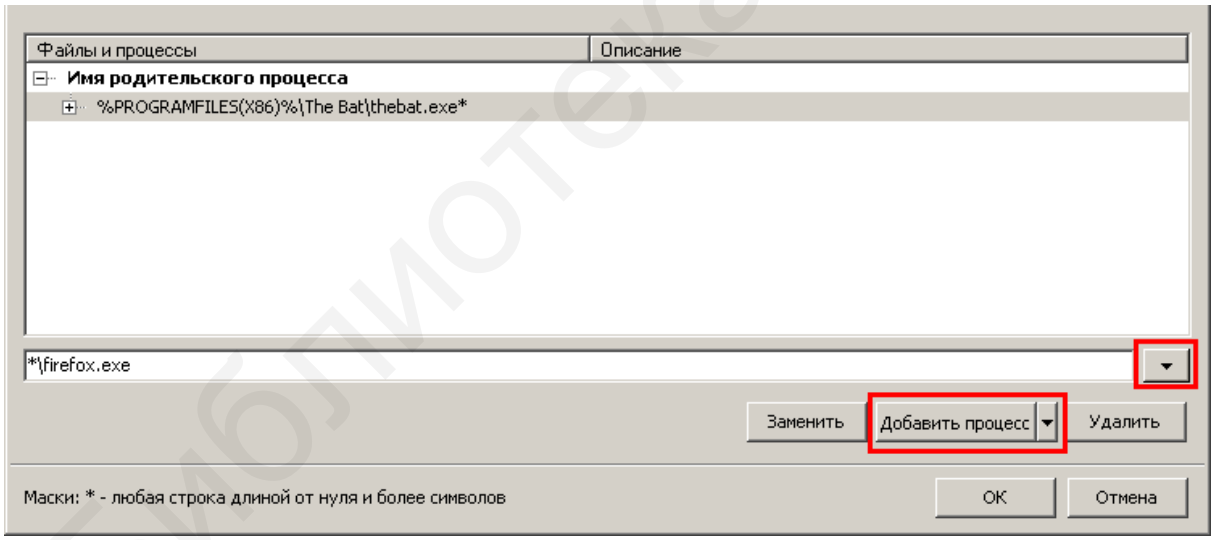


Рис. 2.72. Добавление процессов, для блокировки буфера обмена

Агент DeviceSniffer и «белый список». Находящиеся в «белом списке» внешние устройства исключаются из зоны действия агента DeviceSniffer: пользователь сможет либо иметь к ним полный доступ, либо использовать их в режиме «только чтение». Внешние устройства можно как добавлять, так и исключать из «белого списка». Работа со списком устройств производится на вкладке «Белый список» окна редактирования агента DeviceSniffer (рис. 2.73).

Установленные флажки в строках «Применять настройки теневого копирования» и «Применять настройки блокировки доступа» включают глобальные

Библиотека БГУИР

правила теневого копирования и блокировки доступа, определенные на вкладке «Настройки». Глобальные правила применяются к устройствам, для которых шифрование отключено.

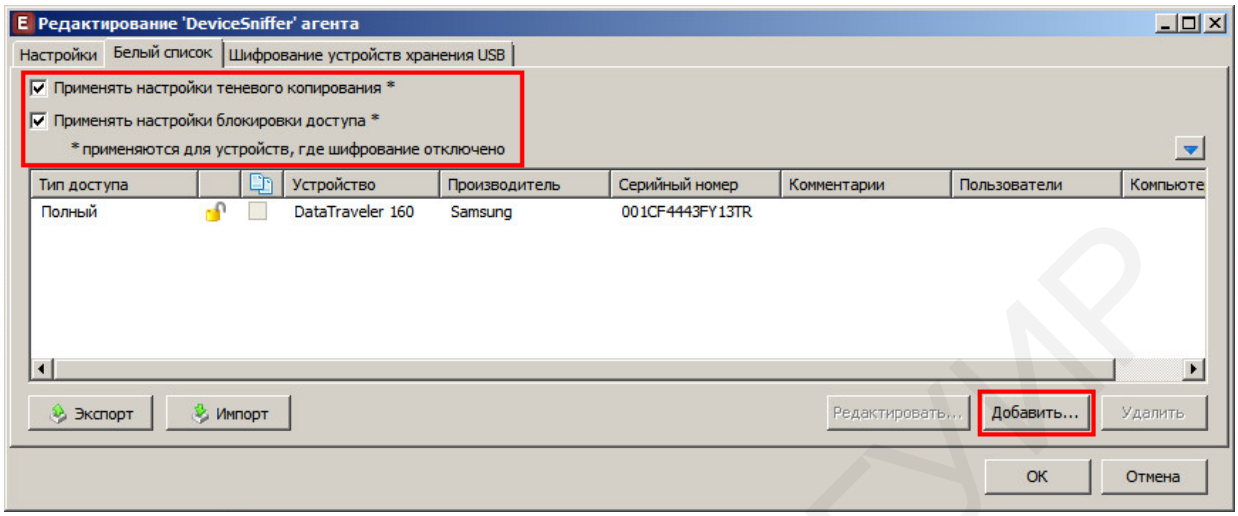


Рис. 2.73. Окно редактирования «белого списка» агента DeviceSniffer

Для добавления внешнего устройства в список нажмите кнопку «Добавить». Выберите тип доступа («полный» либо «только чтение»), задайте параметры шифрования и теневого копирования, введите необходимые данные об устройстве, комментарии, списки пользователей, компьютеров, которые необходимо добавить в «белый список», а также пользователей с разрешением/блокировкой доступа к зашифрованным данным (при отмеченной флажком строке «Шифрование устройств хранения USB») и нажать «OK» (рис. 2.74).

Для включения/отключения шифрования к правилам теневого копирования/доступа используются значки (рис. 2.75):

– шифрование включено;

– шифрование выключено.

Библиотека БГУИР

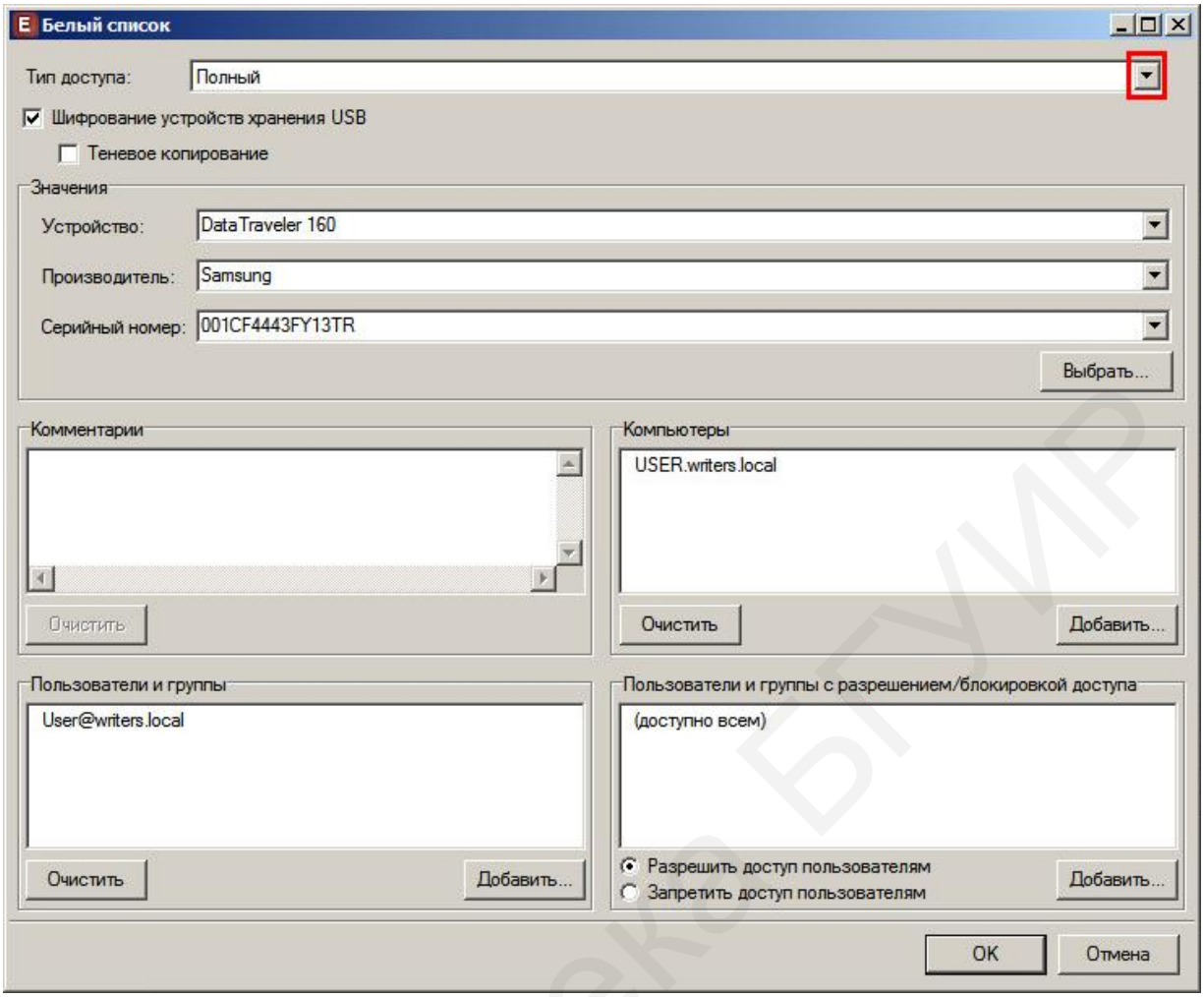


Рис. 2.74. Добавление устройства в «белый список»

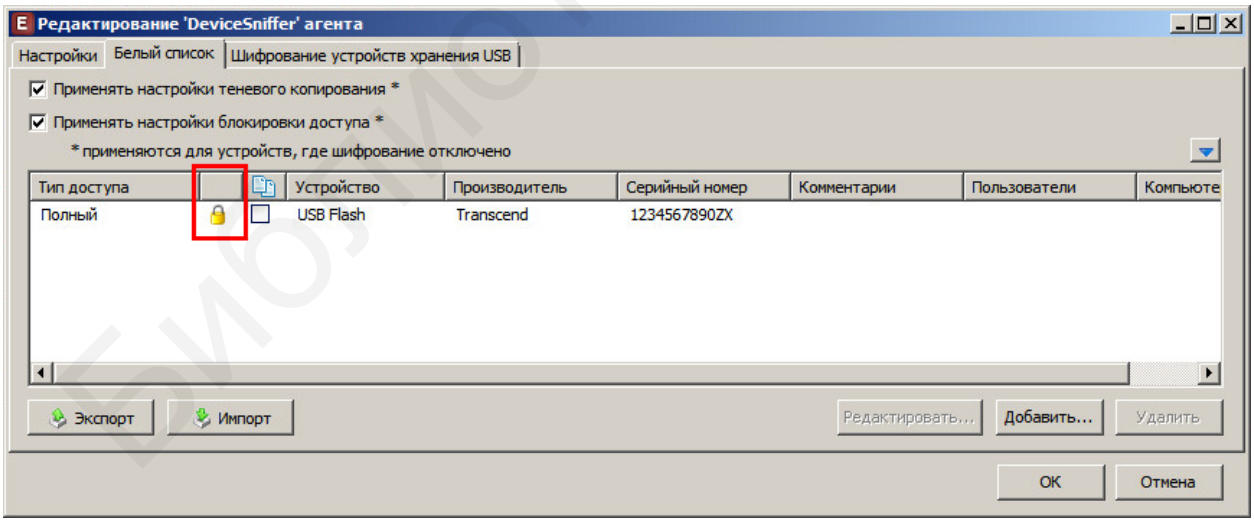


Рис. 2.75. Включение/отключение шифрования

Шифрование данных, записываемых на USB Flash. Использование шифрования позволяет предотвратить возможную утечку данных в случае утери flash-носителя, т. к. просмотреть записанную информацию сможет только пользователь с разрешенным доступом. Также шифрование может

Библиотека БГУИР

использоваться в качестве меры повышения безопасности записи и передачи конфиденциальной информации.

Настройка шифрования позволяет задать различные правила (рис. 2.76). В каждом отдельном правиле можно задать пользователей (группу), записываемые данные которых будут зашифрованы, а также пользователей (группу), доступ к зашифрованным данным для которых будет либо разрешен, либо заблокирован. Для включения шифрования необходимо перейти к настройкам агента DeviceSniffer, выбрать вкладку «Шифрование устройств USB» и отметить флажком строку «Включить шифрование».

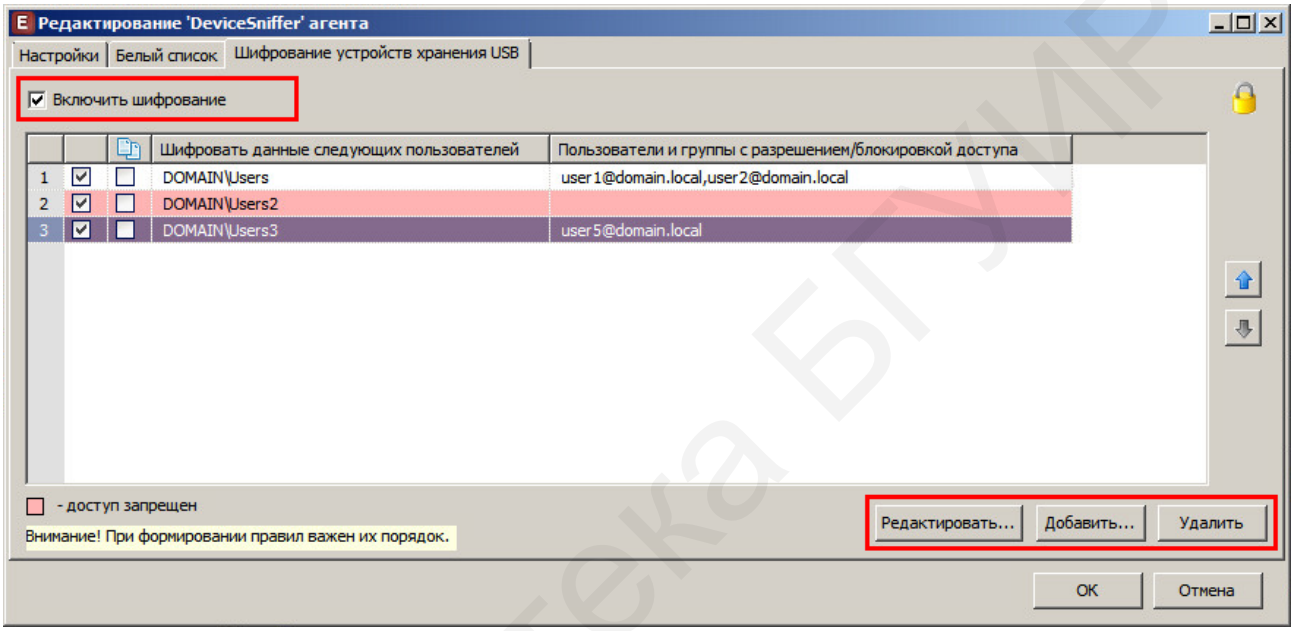


Рис. 2.76. Настройка правил шифрования

В открывшемся окне установите флажок в строке «Включить шифрование». Параметр доступен только для типа доступа «Полный». Для задания правил шифрования используется кнопка «Настройка».

В диалоговом окне «Настройки шифрования» отображается настроенный перечень правил. Для управления списком используются следующие кнопки:

– «Добавить» – создание нового правила;

– «Редактировать» – изменение имеющегося в списке правила;

– «Удалить» – удаление правила из списка.

Нажмите кнопку «Добавить». Появится диалоговое окно «Редактирование правил шифрования» (рис. 2.77).

Работа со списком пользователей, записываемые данные которых будут подвергаться шифрованию, производится в левой части окна. Добавленным в данный список пользователям доступ к зашифрованным данным разрешен по умолчанию.

Работа со списком пользователей, для которых доступ к зашифрованным данным будет разрешен/запрещен, производится в правой части окна.

Библиотека БГУИР

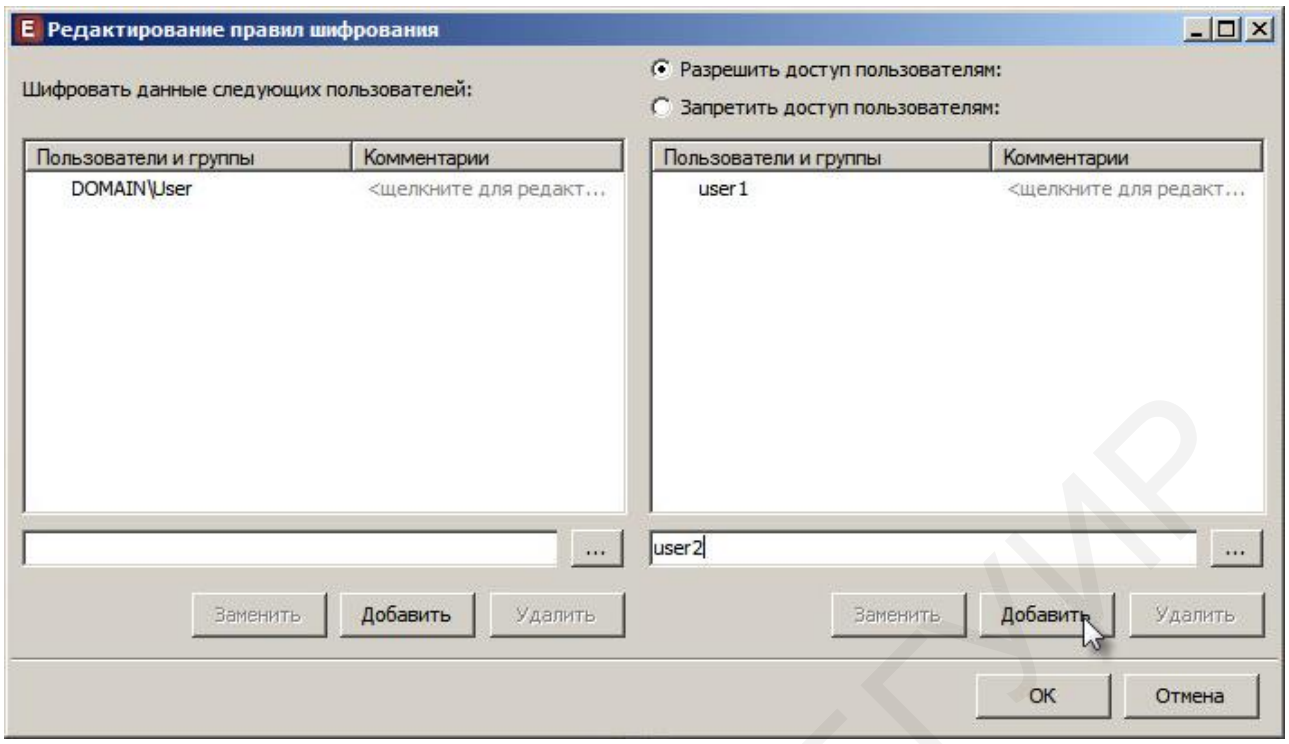


Рис. 2.77. Добавление пользователей

Имя пользователя (группы) можно ввести в текстовое поле вручную:

– ввод имени группы осуществляется в формате DOMAIN\group;

– ввод имени пользователя осуществляется в форматах user@domain.local.

После выбора (ввода) имени пользователя нажмите кнопку «Добавить». По завершении всех настроек нажмите «ОК». Правило будет создано.

2.4.2. Агент FileSniffer

Агент FileSniffer предназначен для контроля операций с файлами, хранящимися на серверах и в общих сетевых папках.

Не рекомендуется включать FileSniffer без предварительной настройки, т. к. в этом случае число перехватываемых данных будет очень большим.

Управление агентом производится на вкладке «Агенты» консоли администрирования. Для доступа к настройкам следует выделить протокол Files и вызвать окно редактирования настроек агента любым из перечисленных способов (рис. 2.78):

– двойным щелчком кнопки мыши по названию протокола;

– нажатием кнопки  в верхней части консоли;

– нажатием кнопки «Дополнительно...».

В окне редактирования агента FileSniffer можно производить настройки по применению аудита операций с файлами к отдельным пользователям, файлам и процессам.

Библиотека БГУИР

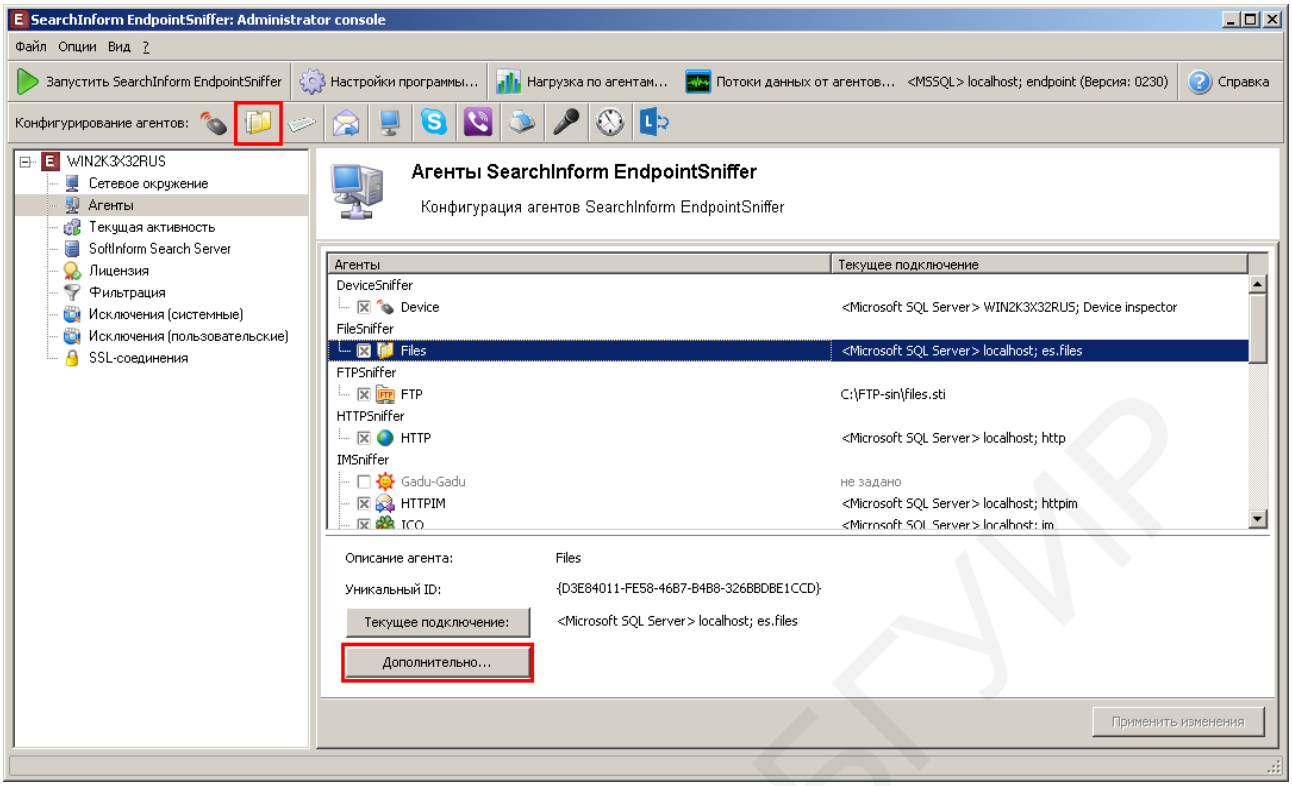


Рис. 2.78. Управление агентом FileSniffer

Применение аудита к пользователям. В диалоговом окне «Редактирование 'FileSniffer' агента» (рис. 2.79) отображается настроенный перечень правил аудита. Для управления списком используются следующие кнопки:

– «Добавить» – создание нового правила аудита;

– «Редактировать» – изменение имеющегося в списке правила;

– «Удалить» – удаление правила из списка.

Работа со списком пользователей, к которым применяется аудит либо которые исключаются из аудита, производится в левой части окна «Добавление правила аудита» (рис. 2.80), которое вызывается нажатием кнопки «Добавить».

Для применения аудита к пользователям из столбца «Пользователи» должен быть выбран фильтр «Аудит только для следующих:». Если выбран исключающий фильтр «Аудит для всех, кроме: », то аудит применяться будет не к выбранным, а, наоборот, ко всем остальным пользователям.

Выбор пользователей, к которым будет применяться аудит, осуществляется аналогично действиям, описанным применительно к управлению доступом к внешнему устройству. Имя пользователя (группы) можно ввести в текстовое поле вручную. При этом ввод имени группы осуществляется в формате DOMAIN\user; ввод имени пользователя – в формате user@domain.local.

После выбора (ввода) имени пользователя необходимо нажать кнопку «Добавить». Для импорта пользователя следует нажать кнопку ..., в открывшемся окне выбрать способ получения списка пользователей (из DataCenter, Active Directory либо NetBIOS), при помощи флажков – пользователей в домене, после чего нажать кнопку «Добавить».

Библиотека БГУИР

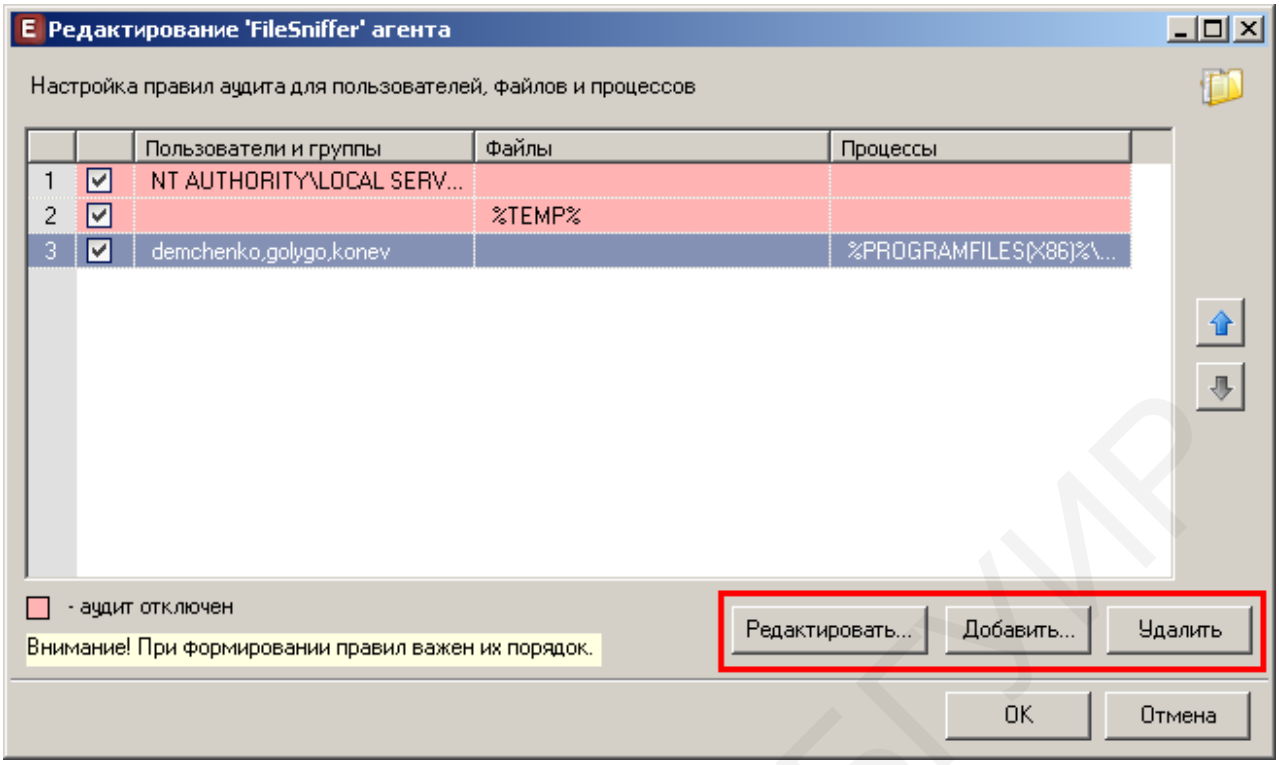


Рис. 2.79. Редактирование настроек агента FileSniffer

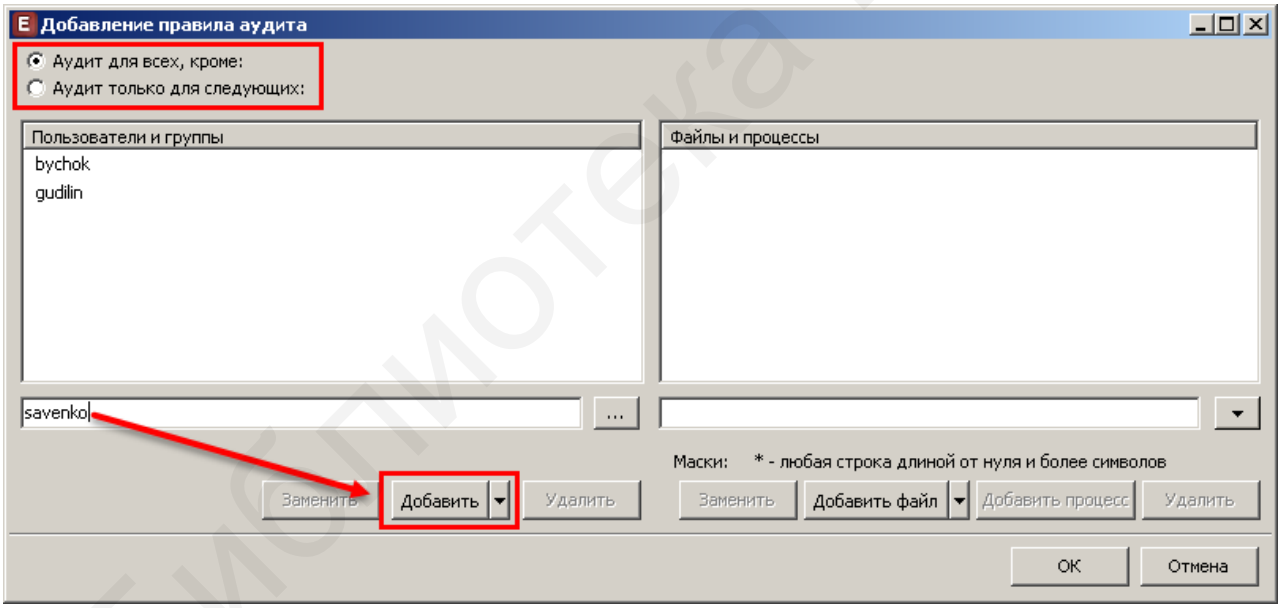


Рис. 2.80. Формирование списка пользователей,
к которым не будет применяться аудит

Если список пользователей достигает больших размеров, можно воспользоваться поиском/фильтрацией. Для этого необходимо ввести запрос в строку «Поиск» и при помощи кнопки «Начинающийся с …» или «Содержащий …» определить, в какой части значения атрибута искать введенное значение.

Для замены одного пользователя другим либо прекращения его аудита следует воспользоваться кнопками «Заменить»/«Удалить».

Библиотека БГУИР

Применение команды «Очистить» из контекстного меню позволяет удалить весь список добавленных в правило пользователей, а не только выделенного пользователя.

Подтверждение изменений, внесенных в список пользователей, производится при помощи нажатия кнопки «ОК» в окне редактирования правила аудита. Рекомендуется добавить системных пользователей к числу исключаемых из аудита, чтобы не вести учет операций (с файлами), совершаемых системой.

Применение аудита к файлам и процессам. Работа со списком файлов и процессов, к которым применяется аудит либо которые исключаются из аудита, производится в правой части окна «Добавление правила аудита» (рис. 2.81).

Для применения аудита к файлам/процессам из столбца «Файлы и процессы» должен быть выбран фильтр «Аудит только для следующих:». Если выбран исключающий фильтр «Аудит для всех, кроме: », то к указанным файлам/процессам аудит применяться не будет (он будет применяться ко всем остальным файлам и процессам).

При отсутствии файла/процесса в списке следует ввести его имя в текстовое поле вручную, после чего нажать кнопку «Добавить файл» либо «Добавить процесс» соответственно.

Помимо применения аудита к отдельным файлам FileSniffer позволяет управлять аудитом отдельных типов файлов, а также аудитом содержимого сетевых папок. Для применения аудита к отдельным типам файлов необходимо щелкнуть по управляющей стрелке в строке «Добавить файл» и выбрать «По имени...».

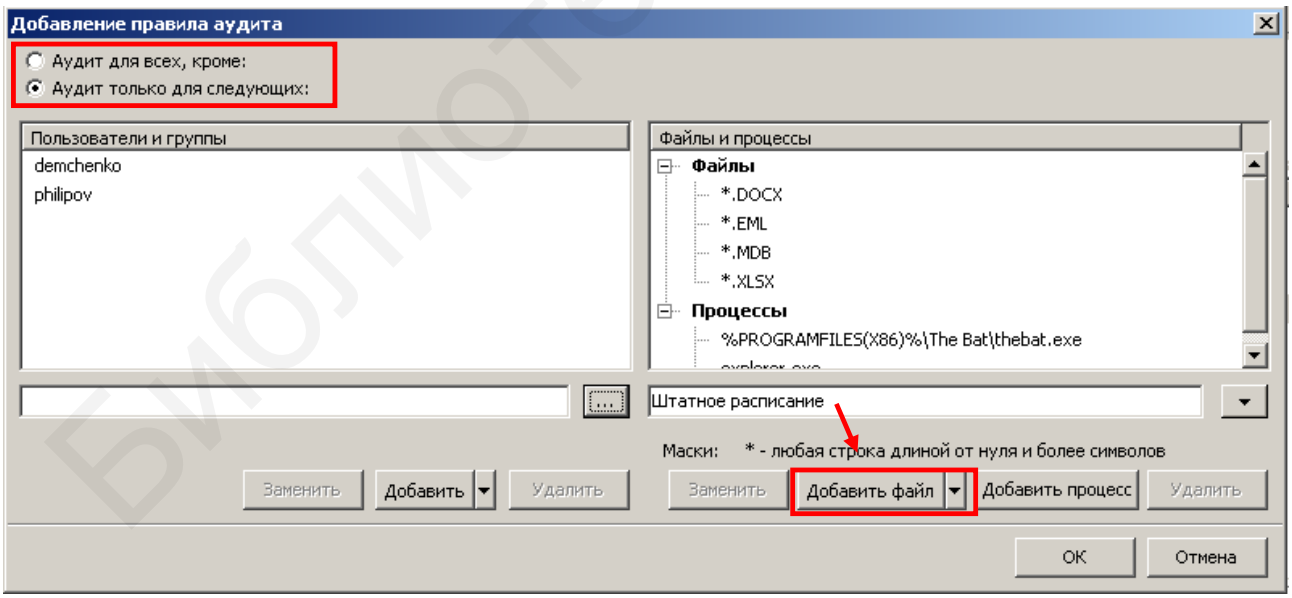


Рис. 2.81. Формирование списка файлов/процессов,
к которым будет применяться аудит

В открывшемся окне «Типы файлов» (рис. 2.82) устанавливаются флажки напротив тех типов файлов, к которым должен применяться аудит.

Библиотека БГУИР

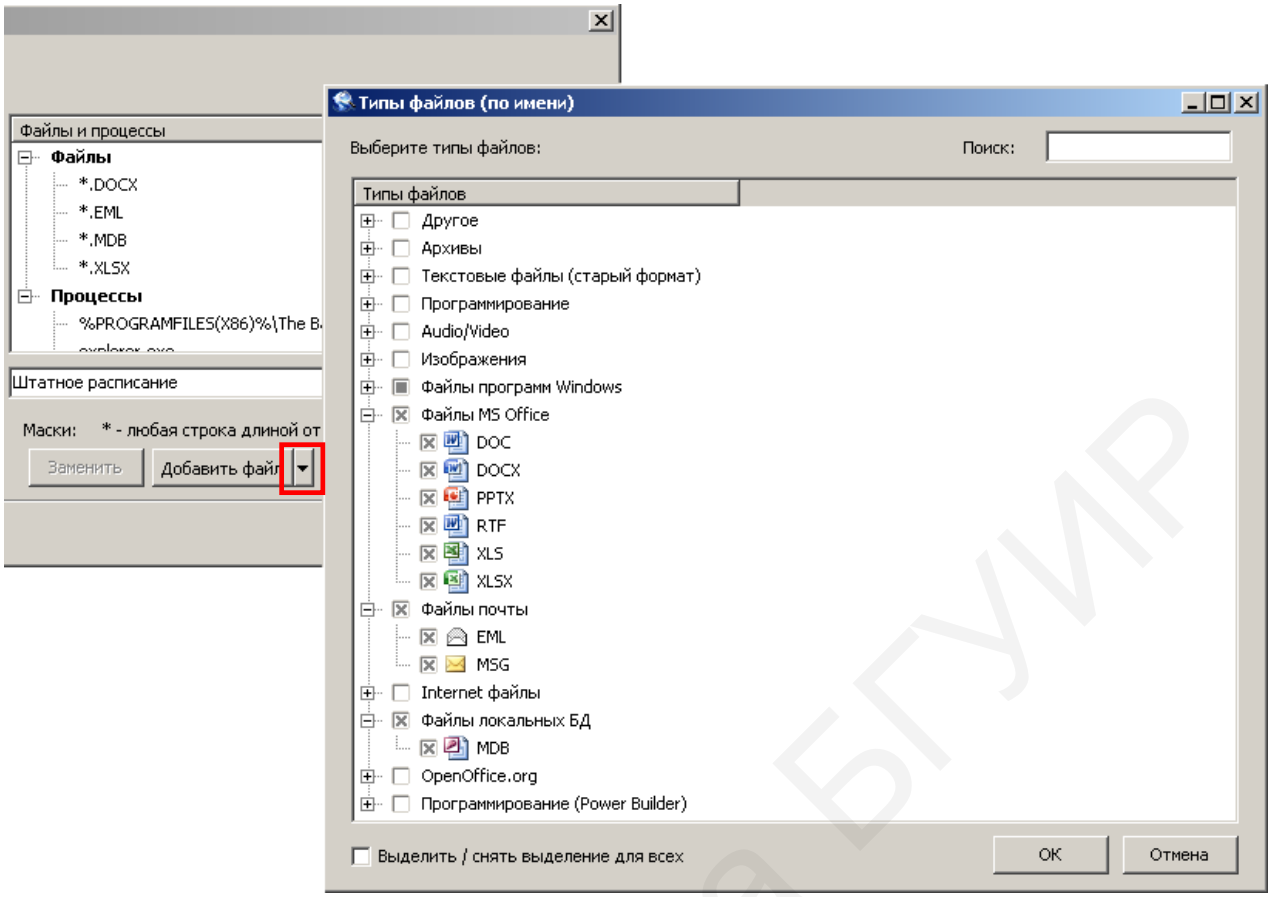


Рис. 2.82. Выбор типов файлов, к которым будет применяться аудит

При помощи флажка в строке «Выделить / снять выделение для всех» можно выполнить соответствующие операции для всех типов файлов одновременно. После нажатия кнопки «OK» произведенный выбор будет сохранен.

Для применения аудита к общим сетевым ресурсам следует щелкнуть по управляющей стрелке в строке «Добавить файл» и выбрать пункт «Сетевые папки». После нажатия кнопки «OK» FileSniffer распространит аудит на операции с файлами, хранящимися в общих сетевых папках.

Также можно использовать предопределенные пути для файлов и процессов, нажав кнопку справа от текстового поля (рис. 2.83).

Для замены файла (типа файла, процесса) другим либо прекращения в отношении его аудита используются кнопки «Заменить»/«Удалить».

Библиотека БГУИР

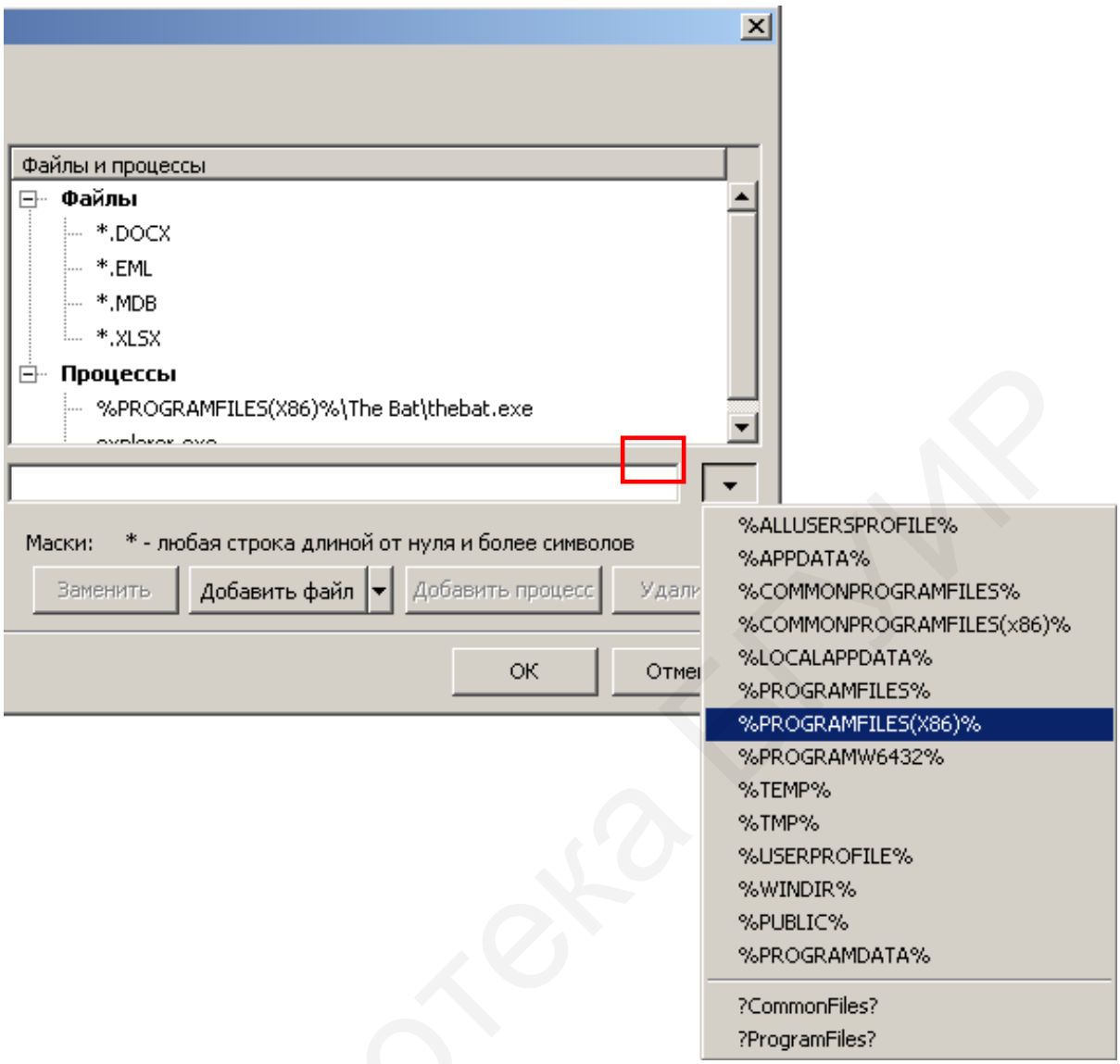


Рис. 2.83. Использование предопределенных путей для файлов и процессов, к которым будет применяться аудит

Применение команды «Очистить» из контекстного меню позволяет удалить весь список добавленных в правило файлов и процессов, а не только выделенную позицию.

Для сохранения настроек необходимо нажать кнопку «OK» в окнах редактирования правила и списка всех правил аудита, а затем – кнопку «Применить изменения» в консоли администрирования EndpointSniffer, чтобы произведенные настройки агента FileSniffer вступили в силу.

Агент HTTPSniffer позволяет перехватывать POST-запросы, отправляемые пользователями при помощи веб-форм. Веб-формы используются для отправки информации в форумы, блоги, чаты, файлообменные службы и другие веб-сервисы.

Управление агентом производится на вкладке «Агенты» консоли администрирования. Выделите протокол HTTP и двойным щелчком кнопки мыши откройте окно редактирования агента либо используйте кнопку «Дополнительно».

Библиотека ГГТУ им. П.О. Сухого

Окно редактирования агента HTTPSniffer позволяет производить настройку минимального размера перехватываемых данных (рис. 2.84).

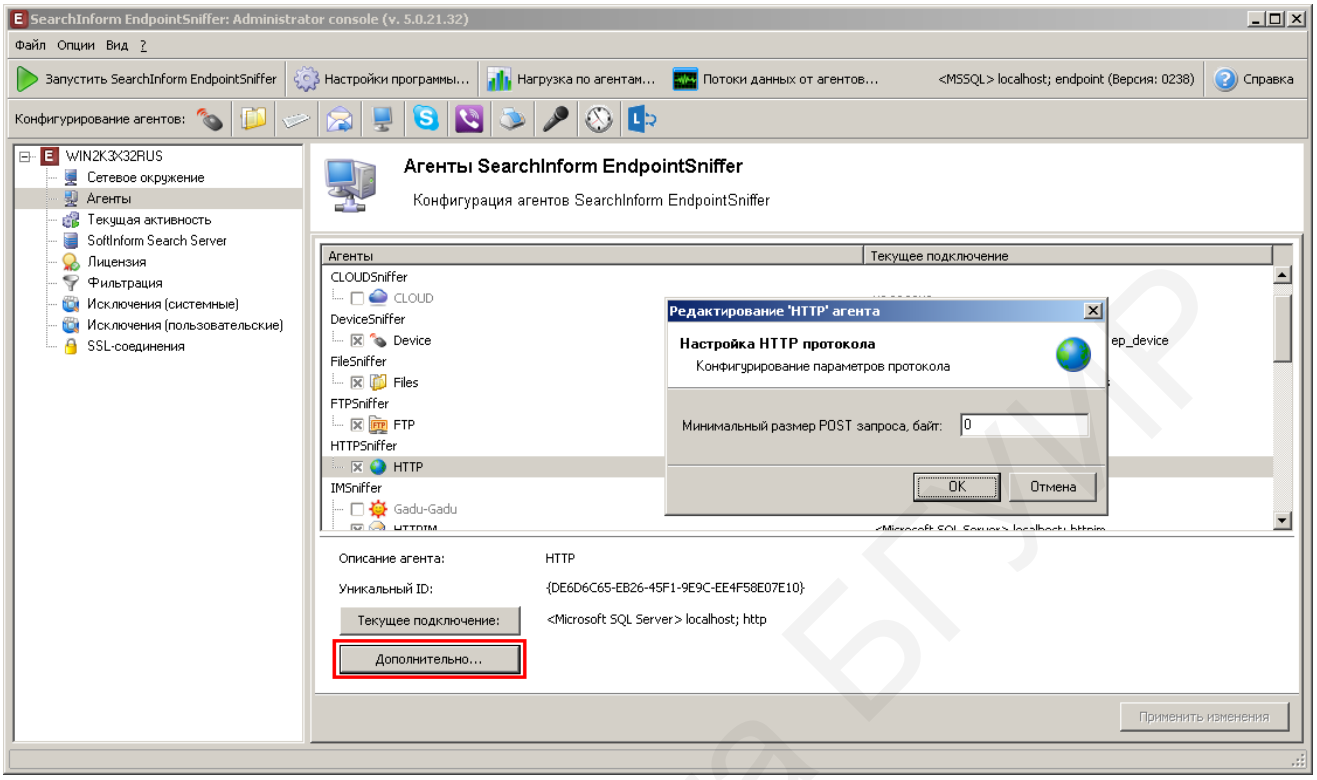


Рис. 2.84. Настройка агента HTTPSniffer

Агент IMSniffer предназначен для контроля сервисов мгновенных сообщений. В настоящей версии компонент IMSniffer поддерживает перехват данных по следующим протоколам: ICQ; MMP; MSN; XMPP; HTTPIM (социальные сети – Facebook, LinkedIn, В Контакте, Мой Мир@Mail.Ru, Одноклассники, Google+, Мамба.ru, Imo.im, Meebo.com); Gadu-Gadu. Настройка агента IMSniffer предусматривает задание дополнительных параметров для протокола ICQ (рис. 2.85).

Агент KeyloggerSniffer предназначен для фиксирования и сохранения в базу данных нажатий клавиш и их сочетаний в различных приложениях.

Управление агентом производится на вкладке «Агенты» консоли администрирования (рис. 2.86). Выделите протокол KeyLogger и двойным щелчком кнопки мыши откройте окно редактирования агента (варианты: нажать кнопку  или «Дополнительно»).

Библиотека БГУИР

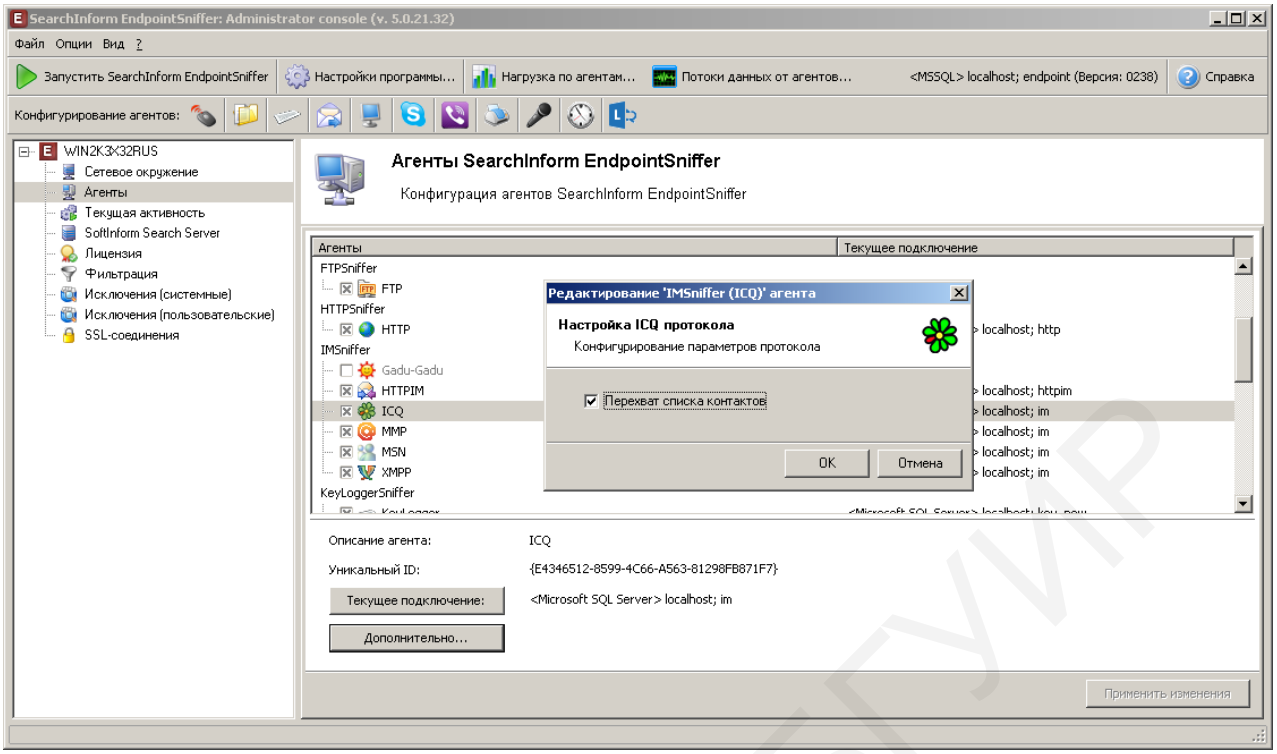


Рис. 2.85. Настройка агента IMSniffer (ICQ)

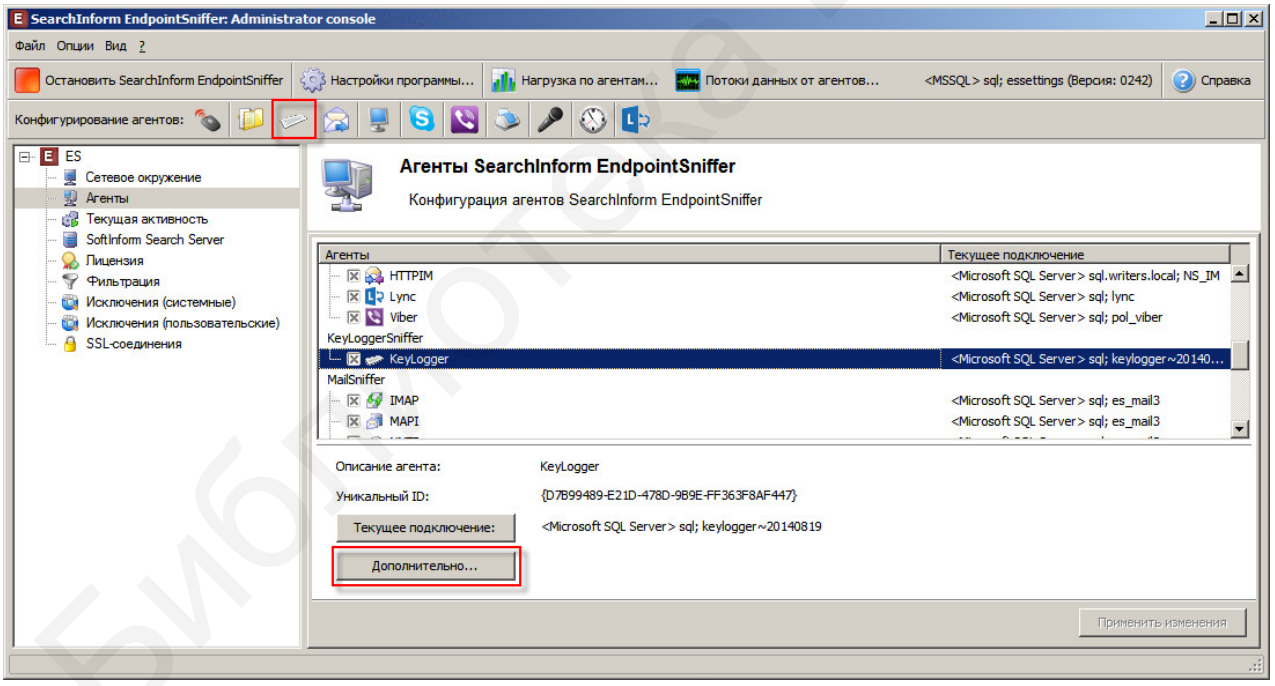


Рис. 2.86. Управление агентом KeyLoggerSniffer

В открывшемся окне редактирования агента KeyLoggerSniffer произведите необходимые настройки по применению перехвата нажатий клавиш к отдельным пользователям и запущенным процессам.

В диалоговом окне «Редактирование 'KeyLogger' агента» (рис. 2.87) отображается настроенный перечень правил перехвата. Для управления списком используются следующие кнопки:

Библиотека БГУИР

– «Добавить» – создание нового правила логирования;
– «Редактировать» – изменение имеющегося в списке правила;
– «Удалить» – удаление правила из списка.

Нажмите кнопку «Добавить».

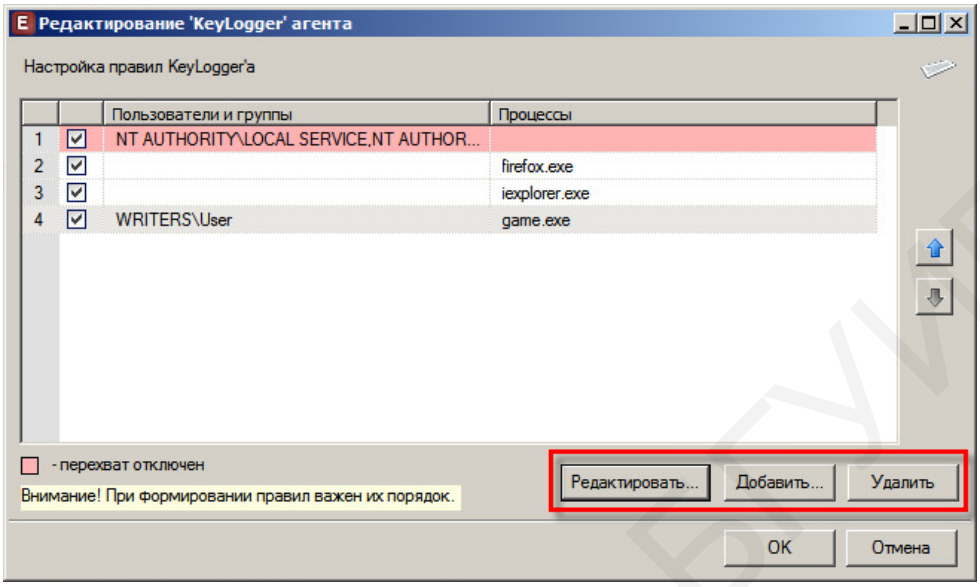


Рис. 2.87. Настройка правил

В открывшемся окне добавления правила для KeyLogger (рис. 2.88) произведите необходимые настройки параметров фильтрации, позволяющей включить в перехват или исключить из него отдельных пользователей, отдельные группы пользователей и процессы.

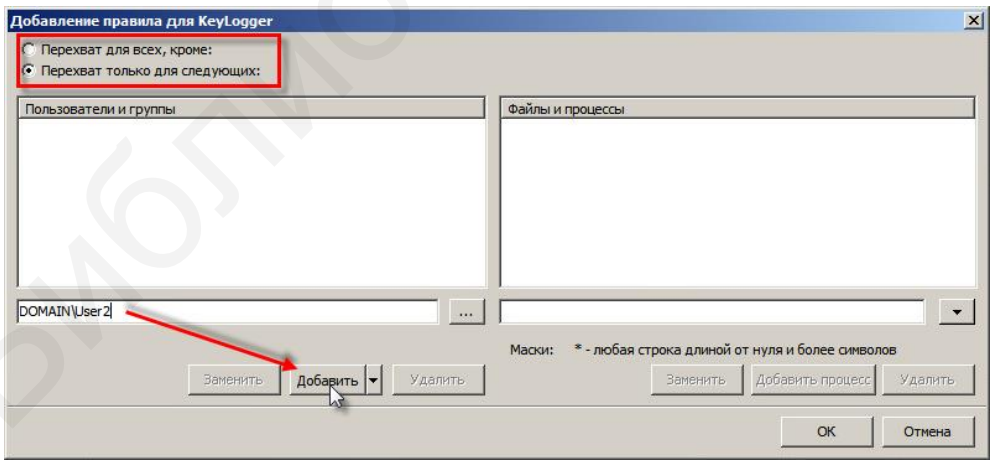


Рис. 2.88. Добавление пользователей

В левой части окна определяется один или несколько пользователей, в правой части – перечень процессов, к которым будут применены одни и те же правила фильтрации (рис. 2.89).

Библиотека БГУИР

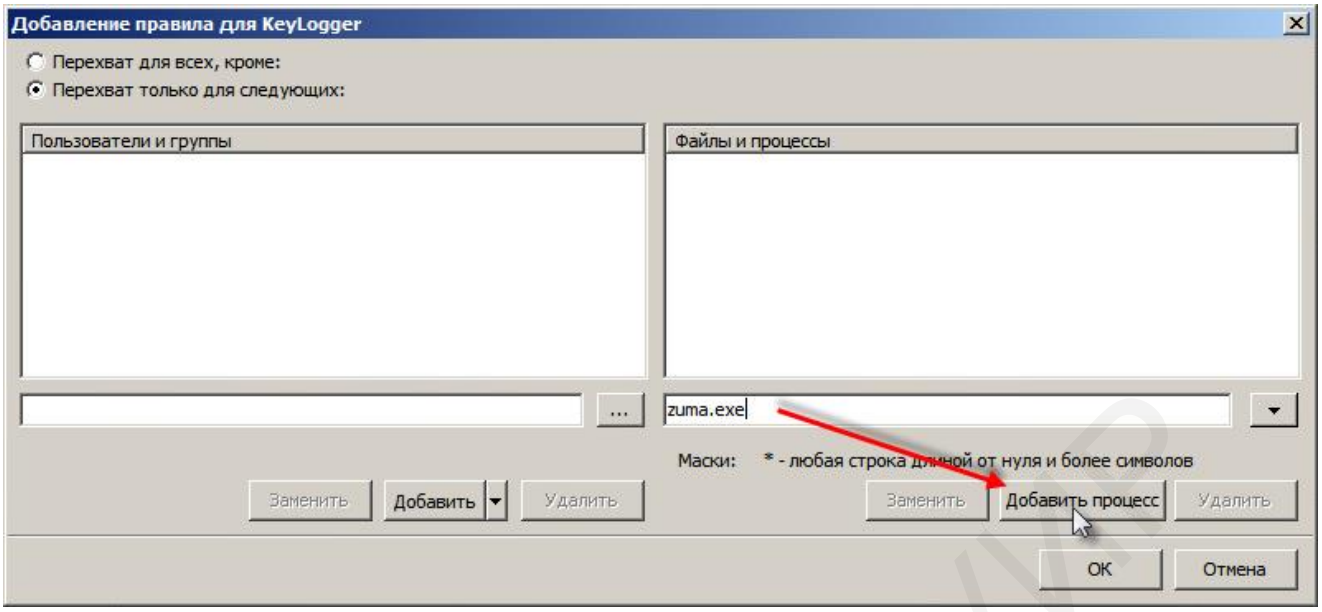


Рис. 2.89. Добавление процесса

Для сохранения настроек нажмите «OK» в окнах редактирования правила и списка всех правил логирования, а затем – кнопку «Применить изменения» в консоли администрирования EndpointSniffer, чтобы произведенные настройки агента KeyLoggerSniffer вступили в силу.

2.4.3. Агент MailSniffer

Агент MailSniffer предназначен для контроля почтового трафика на уровне рабочих станций и сетевых протоколов. Настройка агента MailSniffer предусматривает только одну операцию – включение режима остановки исходящих сообщений электронной почты, передаваемых по протоколу SMTP.

Управление агентом производится на вкладке «Агенты» консоли администрирования. Для доступа к настройкам следует выделить протокол SMTP агента MailSniffer и двойным щелчком кнопки мыши открыть окно редактирования агента (рис. 2.90). Также с этой целью можно воспользоваться кнопкой  или «Дополнительно».

Если необходимо включить блокировку исходящей почты, устанавливается флажок в строке «Блокировать SMTP». При снятом флажке почта блокироваться не будет.

Для сохранения настроек в окне редактирования необходимо нажать кнопку «OK», а затем – кнопку «Применить изменения» на консоли администрирования, чтобы режим остановки исходящих сообщений электронной почты MailSniffer был включен.

Библиотека БГУИР

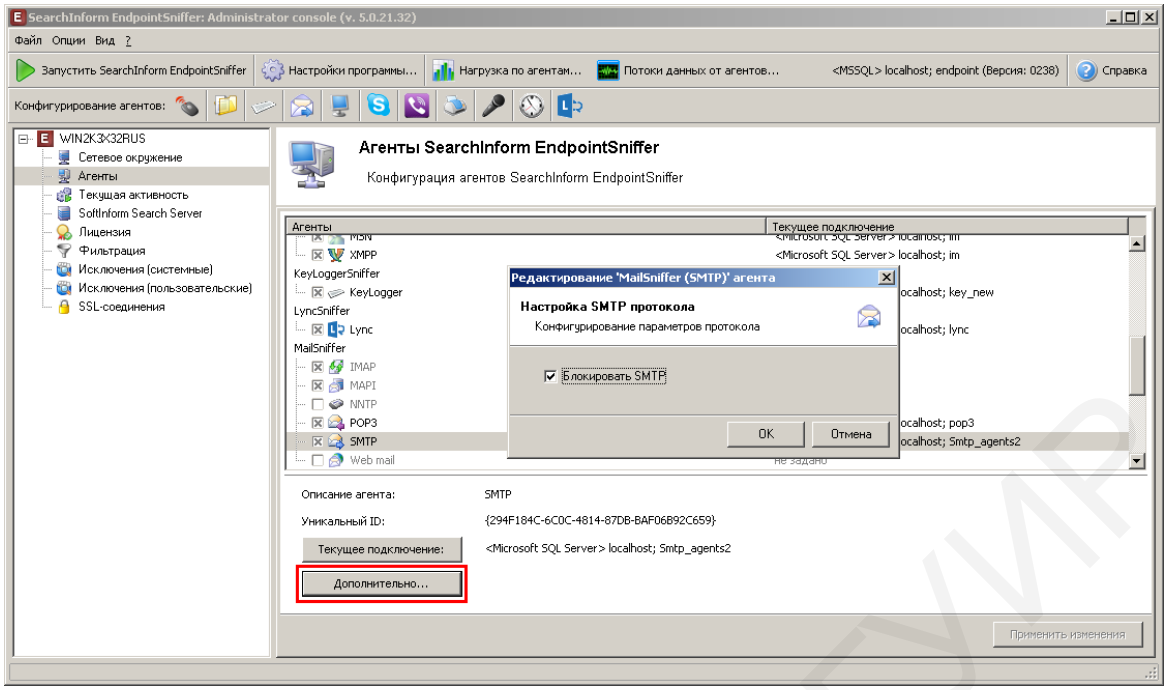


Рис. 2.90. Управление агентом MailSniffer

2.4.4. Агент MicrophoneSniffer

Агент MicrophoneSniffer предназначен для контроля разговоров работников, находящихся как внутри помещений организации/предприятия, так и за их пределами (например, во время деловых встреч, в командировках). Запись голоса выполняется с помощью любого обнаруженного в системе микрофона (в составе гарнитуры, ноутбука, веб-камеры и т. п.).

Управление агентом производится на вкладке «Агенты» консоли администрирования. Для доступа к настройкам следует выделить протокол Microphone и двойным щелчком кнопки мыши открыть окно редактирования агента (рис. 2.91). Также с этой целью можно воспользоваться кнопкой  или «Дополнительно».

Запись речи пользователей может вестись как внутри охраняемого периметра, включающего основные помещения организации/предприятия (вкладка «В офисе»), так и в случае нахождения работника в командировке при наличии у него корпоративного ноутбука (вкладка «Вне офиса») с установленным агентом. Настройки на обеих вкладках идентичны, а режим «Вне офиса» включается автоматически при переходе агента в офлайн.

Настоятельно рекомендуется не оставлять настройки по умолчанию на вкладке «Вне офиса»! В случае, когда агент не может обнаружить сервер управления, он накапливает данные локально на системном диске в ожидании доступности сервера EndpointSniffer, которому можно передать перехваченные данные. При этом если агент настроен на перехват всего подряд, размер очереди на системном диске быстро достигает максимального (указанного) объема, после чего производится циклическая запись, и наиболее старые данные стираются. Назначение имеющихся настроек агента MicrophoneSniffer представлено в табл. 2.3.

Библиотека БГУИР

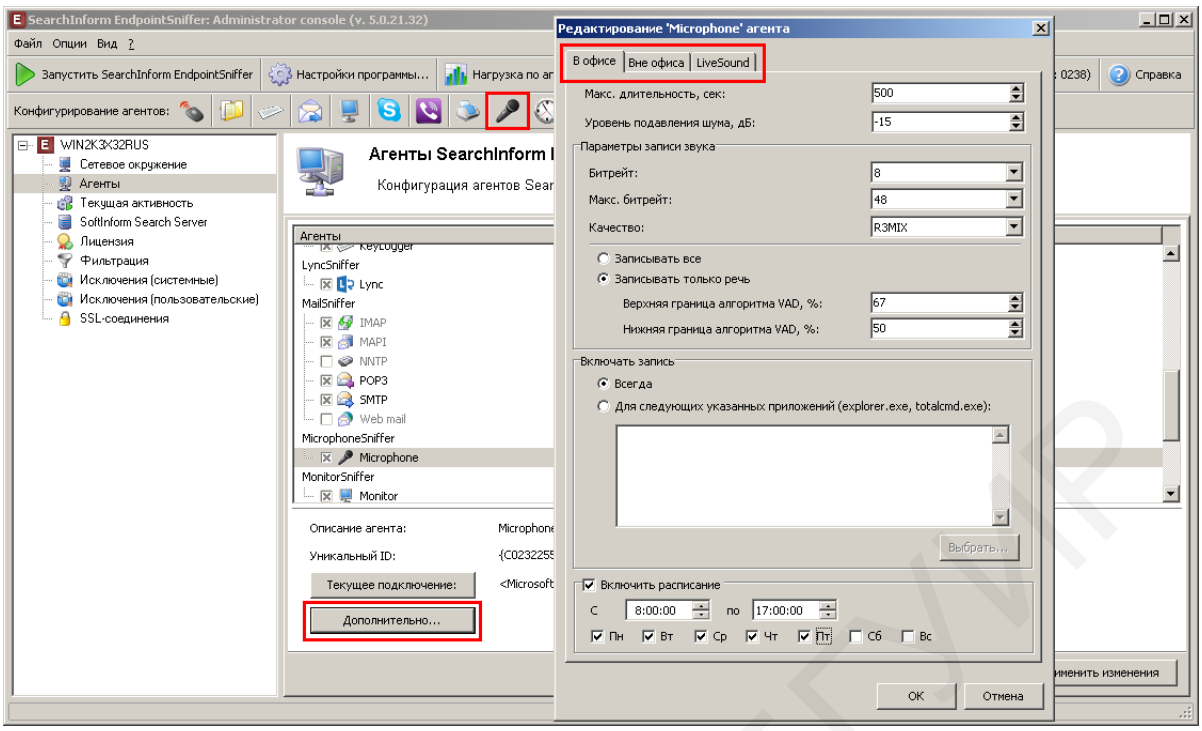


Рис. 2.91. Управление агентом MicrophoneSniffer

Таблица 2.3

Назначение настроек агента MicrophoneSniffer

Параметр (группа параметров)	**Значение**
1	**2**
Вкладки «В офисе» и «Вне офиса»	
Макс. длительность, сек	Ограничение максимальной длительности записываемого файла. Настройка производится в пределах 120–900 с
Параметры записи звука	Агент может перехватывать как все окружающие звуки (параметр «Записывать все»), так и исключительно речь, распознаваемую алгоритмом Voice Activity Detection среди фонового шума или тишины (параметр «Записывать только речь»). При этом можно изменять значения верхней и нижней границ работы алгоритма, тем самым указывая громкость обнаруженной речи, при которой будет производиться перехват
Битрейт	Задается битрейт (величина потока данных, передаваемого в реальном времени): минимальный – 8 кбит/с, максимально возможный – 320 кбит/с
Макс. битрейт	Задается максимальный битрейт
Качество	Параметр позволяет выбрать один из стандартных уровней качества записи сеанса голосовой связи.
Включать запись	Запись может вестись как постоянно (параметр «Всегда»), так и при запуске определенных приложений, перечень которых можно указать в текстовом поле или выбрать с помощью проводника (параметр «Для следующих указанных приложений»)
Включить расписание	При отмеченном флажке задается временной промежуток (начало, окончание, дни недели), в течение которого будет осуществляться перехват

Библиотека БГУИР

Окончание табл. 2.3

1	2
Вкладка «LiveSound»	
Включено	Установленный флажок включает режим LiveSound, снятый – отключает
Порт	Позволяет задавать номер порта, через который производится передача данных в режиме LiveSound. Если порт отличается от значения по умолчанию, то соответствующий номер должен быть задан и в SearchInform Client
Вкладка «Авторизация»	
Не задано	Тип авторизации не задан
Пароль	Позволяет ограничивать доступ к режиму LiveSound, задав пароль. Для разрешения работы в настройках SearchInform Client необходимо подтвердить пароль
Выбранные пользователи	Разрешает добавленным пользователям работать с LiveSound в SearchInform Client. Добавление аналогично описанному в подразделе «Для выбранных»

2.4.5. Агент MonitorSniffer

На рис. 2.92 продемонстрирован порядок управления агентом MonitorSniffer.

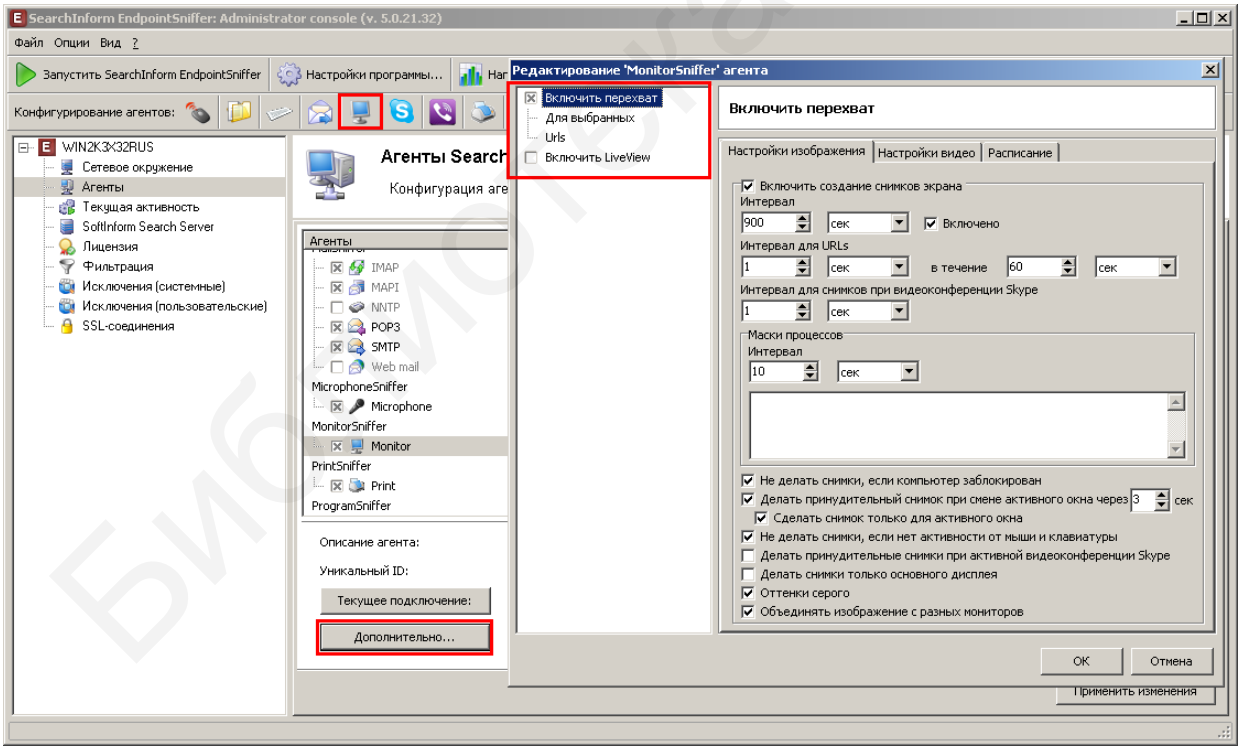


Рис. 2.92. Управление агентом MonitorSniffer

В зависимости от того, к какой группе относится контролируемый объект, используются различные настройки для перехвата, размещенные на следующих вкладках:

– «Для всех» (совпадает с «Включить перехват»);
– «Для выбранных»;
– «URLs».

Для сохранения настроек в окне редактирования необходимо нажать кнопку «OK», а затем – кнопку «Применить изменения» на консоли администрирования, чтобы настройки агента MonitorSniffer вступили в силу.

Настройки агента MonitorSniffer для всех пользователей размещены на вкладке «Включить перехват». В свою очередь вкладка «Включить перехват» содержит следующие внутренние вкладки:
– «Настройки изображения»;
– «Настройки видео»;
– «Расписание».

Описание настроек вкладки «Для всех» (вкладка «Включить перехват») агента MonitorSniffer представлено в табл. 2.4. Назначение настроек, находящихся на вкладках «Настройки изображения», «Настройки видео» и «Расписание» вкладки «Для выбранных» агента MonitorSniffer, не отличается от одноименных настроек, находящихся на вкладке «Для всех».

Описание настроек для вкладки «Пользователи и группы» представлено в табл. 2.5.

Таблица 2.4

Описание настроек вкладки «Для всех» агента MonitorSniffer

Настройка	**Описание**
1	**2**
Вкладка «Настройка изображения»	
Интервал	Позволяет задавать интервал (в секундах, минутах), через который будет происходить захват изображений экрана
Включено	Установленный флажок включает захват содержимого экранов пользователей через заданный интервал
Интервал для URLs	Позволяет задавать интервал (в секундах, минутах) захвата содержимого экранов для заданного URL, а также время (в секундах, минутах), в течение которого такой захват будет происходить. При отсутствии заданного URL (в группе «URLs») нет необходимости в использовании данной настройки
Интервал для снимков видеоконференции Skype	Позволяет задавать интервал (в секундах, минутах), через который будет происходить захват изображений видеоконференции Skype
Маски процессов	Позволяет задавать: – интервал (в секундах, минутах) захвата содержимого экрана применительно к указанным маскам процессов; – процессы, к которым применяются маски. Захват содержимого экранов осуществляется применительно к приложениям, для которых прописаны маски процессов; при этом должно быть запущено хотя бы одно из указанных приложений
Поведение при заблокированном компьютере	Установленный флажок отменяет захват снимков экрана при заблокированном компьютере

Продолжение табл. 2.4

1	2
Поведение при смене активного окна	Установленный флажок включает режим принудительного захвата снимков экрана при смене пользователем активного окна: снятие изображения экрана будет происходить при каждом переходе пользователя в другое окно через заданное число секунд
Сделать снимок только активного окна	При установленном флажке снимается только активное окно. При снятом – весь экран
Поведение при отсутствии активности	Установленный флажок отменяет захват снимков экрана при отсутствии активности пользователя (бездействие мыши и клавиатуры) в течение 10 мин
Поведение при видеоконференции Skype	При установленном флажке будет производиться захват снимков видеоконференции Skype с указанным выше интервалом
Делать снимки только основного дисплея	Если к компьютеру пользователя подключено несколько мониторов, то при установленном флажке снимки будут производиться только с основного дисплея
Оттенки серого	При установленном флажке снимки сохраняются в оттенках серого цвета вместо цветного изображения
Объединять изображения с разных мониторов	При установленном флажке снимки с разных мониторов объединяются в одно изображение
Вкладка «Настройка видео»	
Включить создание видео	Установленный флажок включает видеозапись мониторной активности
Оттенки серого	При установленном флажке видео сохраняется в оттенках серого цвета вместо цветной видеозаписи
Исключить фон	При установленном флажке не записывается фоновое изображение
Использовать зеркальный драйвер для монитора	При включенном параметре пропадает возможность использования темы оформления Windows Aero, при выключенном – увеличивается нагрузка на ресурсы рабочей станции
Поведение при заблокированном компьютере	Установленный флажок отменяет захват видео с экрана при заблокированном компьютере
Сделать снимок только для активного окна	При установленном флажке снимается только активное окно, при снятом – весь экран
Делать снимки только для основного дисплея	Если к компьютеру пользователя подключено несколько мониторов, то при установленном флажке запись видео будет производиться только с основного дисплея
Объединять видео с разных мониторов	При установленном флажке видео с разных мониторов объединяется в один файл
Дополнительные настройки	При установленном флажке доступна корректировка частоты кадров в секунду. Рекомендуемое значение – 10 кадров/с. При заданных рекомендуемых параметрах объем данных в БД в среднем составит 50–400 МБ (варьируется в зависимости от выполняемых пользователем действий) с одного компьютера за рабочий день

Библиотека БГУИР

Окончание табл. 2.4

1	2
Вкладка «Расписание»	
Включение расписания	Установленный флажок включает режим захвата изображений экрана по заданному расписанию
Время	Задает начальное и конечное время, в течение которого будет производиться захват снимков экрана. Требуемые значения вводятся вручную либо выбираются с помощью регулятора
Дни недели	Задает дни недели, по которым будет производиться захват снимков экрана. Дни недели назначаются при помощи установки соответствующего флажка

Таблица 2.5

Описание настроек, находящихся на вкладке «Пользователи и группы» вкладки «Для выбранных» агента MonitorSniffer

Настройка	Описание
Вкладка «Пользователи и группы»	
[поле просмотра]	Отображает список пользователей, у которых будет производиться захват снимков экрана. Команда «Очистить» из контекстного меню полностью удаляет список пользователей
[поле ввода]	Позволяет вводить имя пользователя или группы, у которых будет производиться захват снимков экрана
Кнопка добавления пользователей 	Открывает стандартное окно импортирования пользователей. В данном окне можно получить список пользователей с помощью одного из трех источников: – модуль DataCenter; – каталог Active Directory; – каталог NetBIOS. Получение списка пользователей осуществляется аналогично действиям, описанным применительно к управлению доступом к внешнему устройству или процессам
Кнопка «Заменить»	Позволяет заменить пользователя или группу из списка на пользователя или группу, указанные в поле ввода
Кнопка «Добавить»	Позволяет добавить пользователя или группу, у которых будет производиться захват снимков экрана
Кнопка «Удалить»	Позволяет удалить пользователя или группу, у которых будет производиться захват снимков экрана

Настройки агента MonitorSniffer для выбранных пользователей размещены на вкладке «Для выбранных» (рис. 2.93), которая содержит следующие внутренние вкладки:

– «Настройки изображения»;

– «Настройки видео»;

– «Расписание»;

– «Пользователи и группы».

Настройки агента MonitorSniffer для выбранных единых указателей ресурсов (URL) размещены на вкладке «URLs» (рис. 2.94). Расположенное на ней поле ввода позволяет вводить и просматривать URL. Захват содержимого экра-

Библиотека БГУИР

нов осуществляется только применительно к указанным URL, которые должны быть открыты в браузере.

Ввод URL осуществляется по одному на строку, при этом можно указывать части доменов, например, www.yandex.ru, mail.ru, ru.wikipedia.org/wiki/.

Периодичность, с которой будет происходить захват снимков экрана при открытии пользователем заданных URL, а также длительность процесса захвата настраивается на вкладке «Для всех» или «Для выбранных».

Настройки режима оперативного контроля активности экрана одного или нескольких пользователей (просмотр в режиме реального времени) размещены на вкладке LiveView (рис. 2.95).

Подробное описание настроек режима LiveView представлено в табл. 2.6.

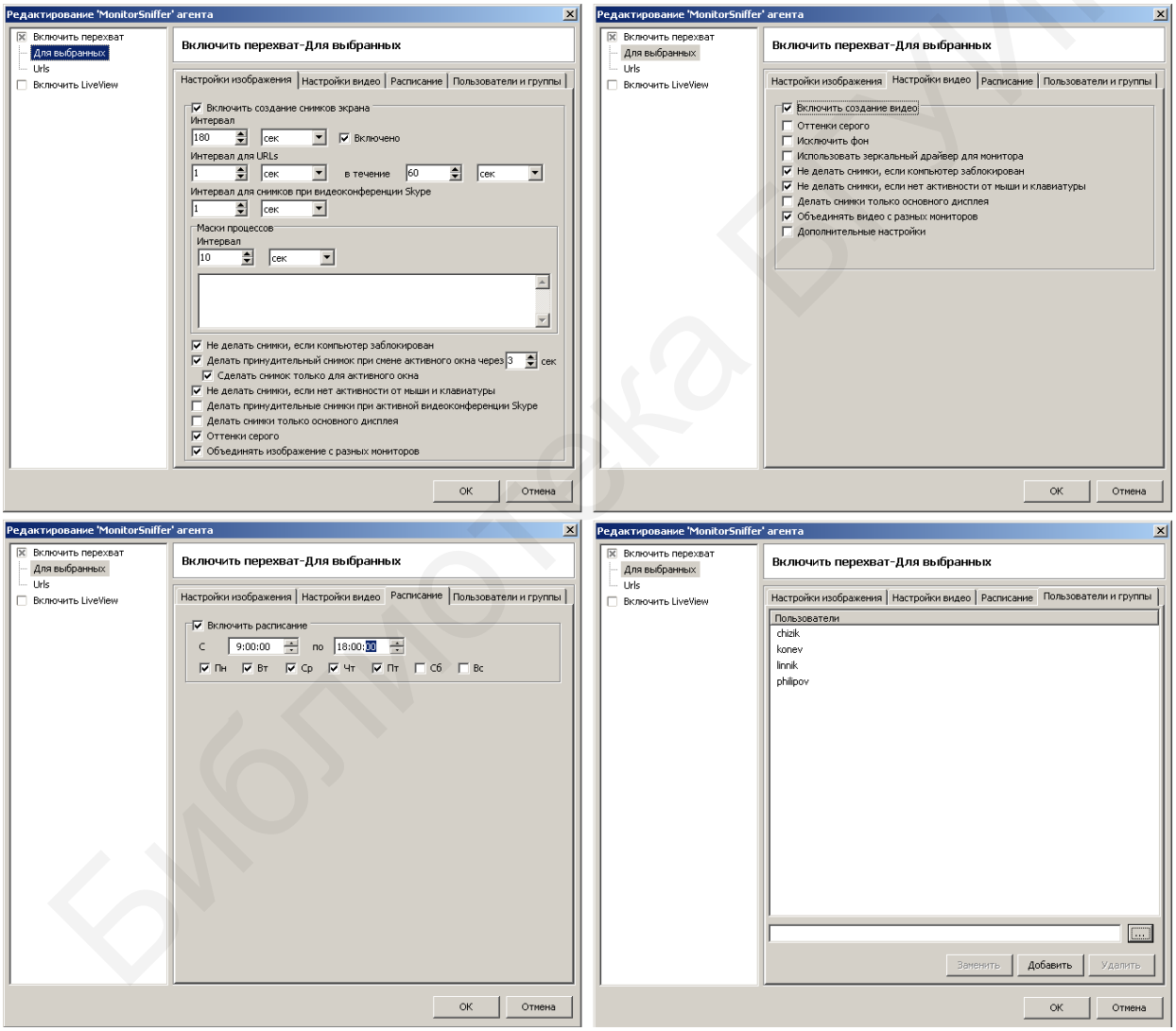


Рис. 2.93. Настройки агента MonitorSniffer для выбранных пользователей

Библиотека БГУИР

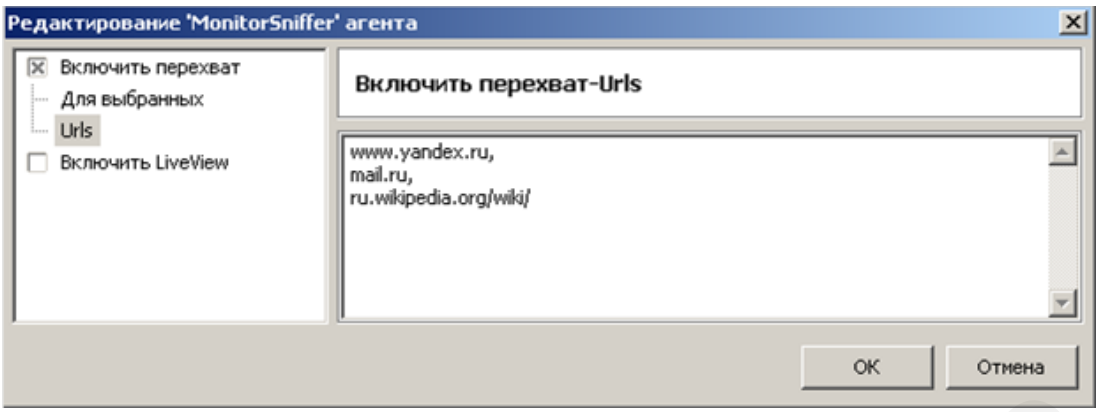


Рис. 2.94. Настройки агента MonitorSniffer
для выбранных единых указателей ресурсов (URL)

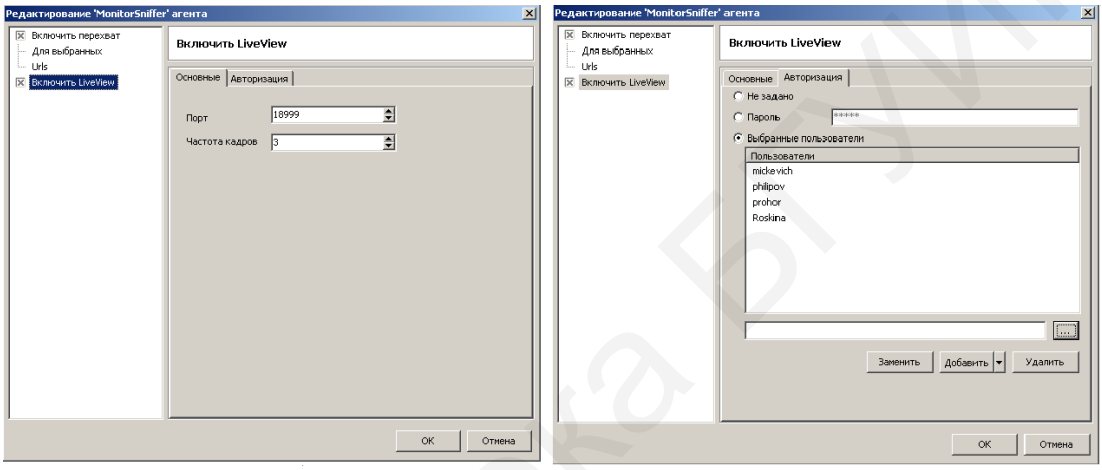


Рис. 2.95. Настройки режима LiveView

Таблица 2.6

Описание настроек режима LiveView

Настройка	Описание
Вкладка «Основные»	
Порт	Позволяет задавать номер порта, через который производится передача данных в режиме оперативного контроля. Если порт отличается от значения по умолчанию, то соответствующий номер должен быть задан и для клиентской части MonitorSniffer
Частота кадров	Позволяет задавать частоту смены кадров в режиме реального времени. При повышении частоты смены кадров увеличивается нагрузка на процессор, что приводит к замедлению рабочих операций компьютера
Вкладка «Авторизация»	
Не задано	Тип авторизации не задан
Пароль	Ограничивает доступ к режиму LiveView можно при помощи пароля. Для разрешения работы с настройками клиентской части MonitorSniffer необходимо подтвердить пароль. В противном случае в окне просмотра экрана в режиме реального времени будет отображаться сообщение «Разрыв соединения (ошибка проверки подлинности)»
Выбранные пользователи	Разрешает добавленным пользователям работать с LiveView в клиентской части MonitorSniffer. Получение списка пользователей осуществляется аналогично действиям, описанным применительно к управлению доступом к внешнему устройству или процессам

Библиотека БГУИР

2.4.6. Агент PrintSniffer

Агент PrintSniffer предназначен для перехвата содержимого документов, отправленных на печать. Управление агентом производится на вкладке «Агенты» консоли администрирования. Для доступа к настройкам следует выделить протокол Print и двойным щелчком кнопки мыши открыть окно редактирования агента (рис. 2.96). Также с этой целью можно воспользоваться кнопкой  или «Дополнительно».

Окно редактирования агента PrintSniffer позволяет конфигурировать списки принтеров. Для этого необходимо выбрать из выпадающего меню нужный тип списка:

– «Исключить из сетевого перехвата» – для принтеров из этого списка не перехватываются документы, отправленные на печать;

– «Блокировка Escape функций» – для принтеров из данного списка блокируется печать через функции Escape.

Добавление в список «Блокировка Escape функций» может использоваться для PostScript/PCL-принтеров, на которых не происходит перехват документов. Включение для них блокировки в большинстве случаев позволит перехвату заработать.

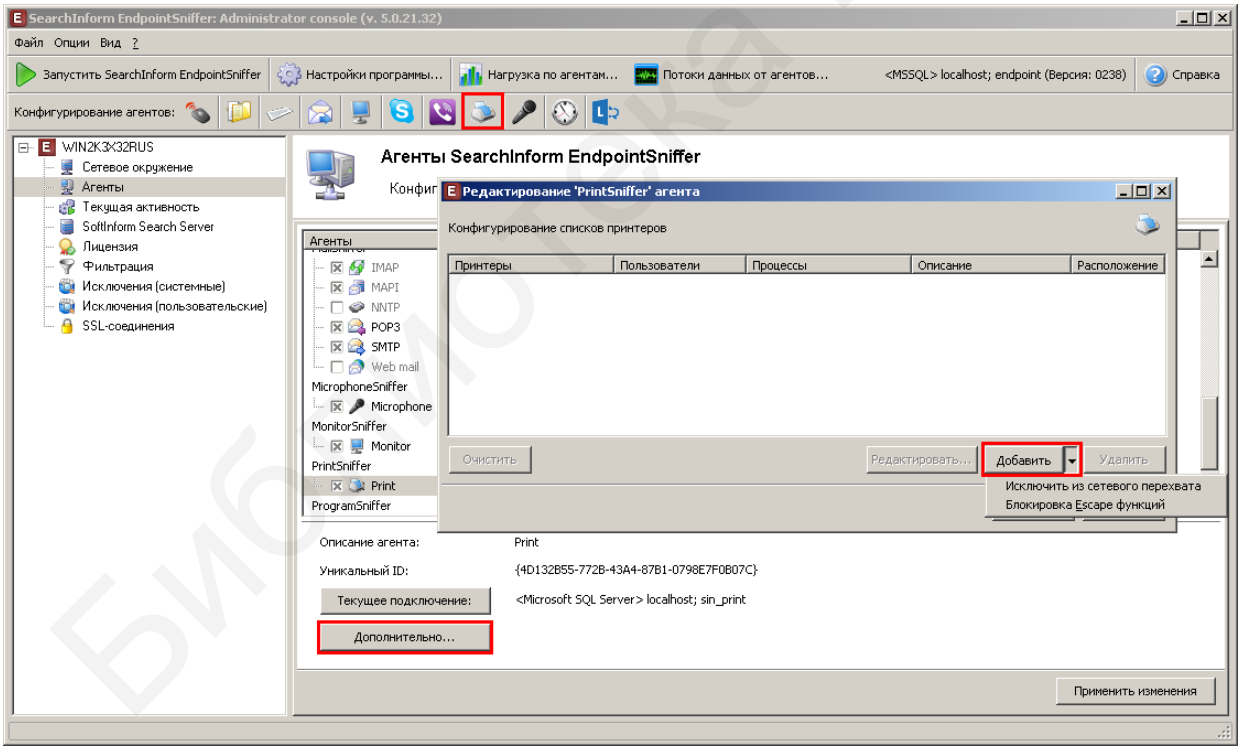


Рис. 2.96. Управление агентом PrintSniffer

Введите название принтера (для выбора всех принтеров введите «*»).

Для типа списка «Исключить из сетевого перехвата» пустое поле в строке «Имя» означает разрешить перехват для принтеров, которые подпадают под заданные ниже параметры, а именно:

Библиотека БГУИР

– «Пользователи» (формат записи для добавления пользователей – user@domain.local, для добавления группы – DOMAIN\group);

– «Процессы»;

– «Описание»;

– «Расположение».

Для завершения добавления принтера нажмите кнопку «ОК» (рис. 2.97).

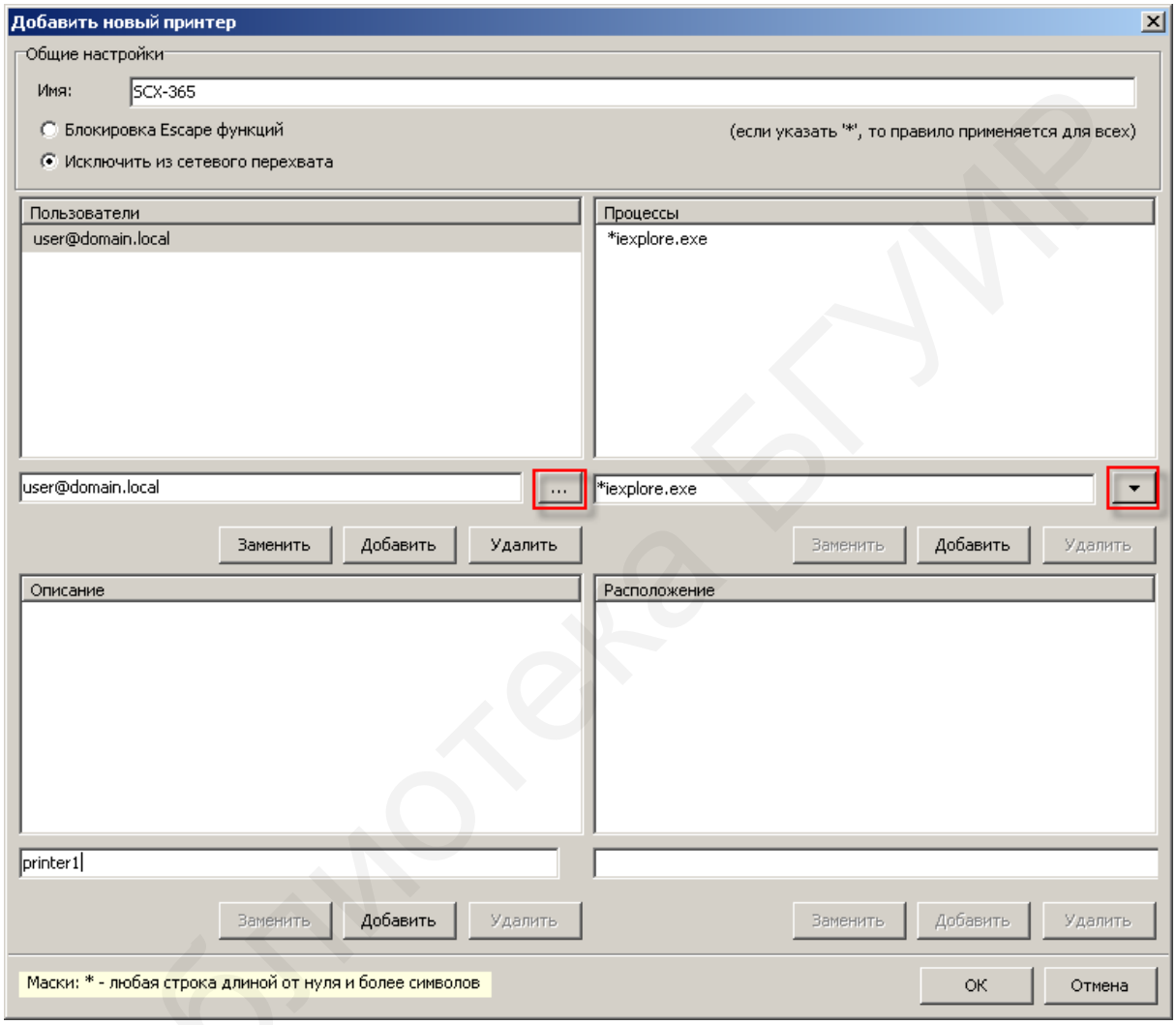


Рис. 2.97. Добавление принтера

Для сохранения настроек в окне редактирования также необходимо нажать «ОК», после чего – кнопку «Применить изменения» на консоли администрирования.

2.4.7. Агент SkypeSniffer

Агент SkypeSniffer предназначен для перехвата и анализа трафика Skype: сеансов текстовой и голосовой связи, а также файлов и SMS-сообщений, переданных при помощи Skype. Управление агентом производится на вкладке «Агенты» консоли администрирования. Для доступа к настройкам следует выделить протокол Skype и двойным щелчком кнопки мыши открыть окно редак-

Библиотека БГУИР

тирования агента (рис. 2.98). Также с этой целью можно воспользоваться кнопкой  или «Дополнительно».

Окно редактирования агента SkypeSniffer позволяет производить настройки фильтрации каналов данных, импорта и параметров голосовой связи. Для этого необходимо установить необходимые флажки либо выбрать из выпадающих списков необходимые значения, для сохранения настроек в окне редактирования нажать кнопку «OK», а затем – кнопку «Применить изменения» на консоли администрирования, чтобы настройки агента SkypeSniffer вступили в силу. Подробное описание настроек агента SkypeSniffer представлено в табл. 2.7.

Таблица 2.7

Описание настроек агента SkypeSniffer

Настройка	**Описание**
Группа «Фильтрация»	
Чаты	Установленный флажок включает перехват чатов
Файлы	Установленный флажок включает захват файлов, переданных через Skype
Звонки	Установленный флажок включает перехват сеансов голосовой связи
SMS	Установленный флажок включает захват отправленных SMS-сообщений
Группа «Импорт»	
Чаты	Установленный флажок позволяет перехватывать историю сообщений в чатах
SMS	Установленный флажок позволяет сохранять историю отправленных SMS-сообщений
Группа «Звук»	
Битрейт	Задается битрейт: минимальный – 8 кбит/с, максимально возможный – 320 кбит/с
Макс. битрейт	Задается максимальный битрейт
Качество	Задается уровень качества записываемого сеанса голосовой связи
Метод захвата	Задается метод захвата звука: DirectSound; Skype API; Использовать все
Макс. длительность, сек	Устанавливается максимальная длительность сеанса голосовой связи
Группа «Skype пользователи»	
Перехват для всех, кроме:	Задаются логины пользователей Skype (через запятую), которые будут исключены из перехвата
Перехват только для следующих:	Задаются логины (через запятую) только тех пользователей Skype, для которых будет осуществляться перехват

Библиотека БГУИР

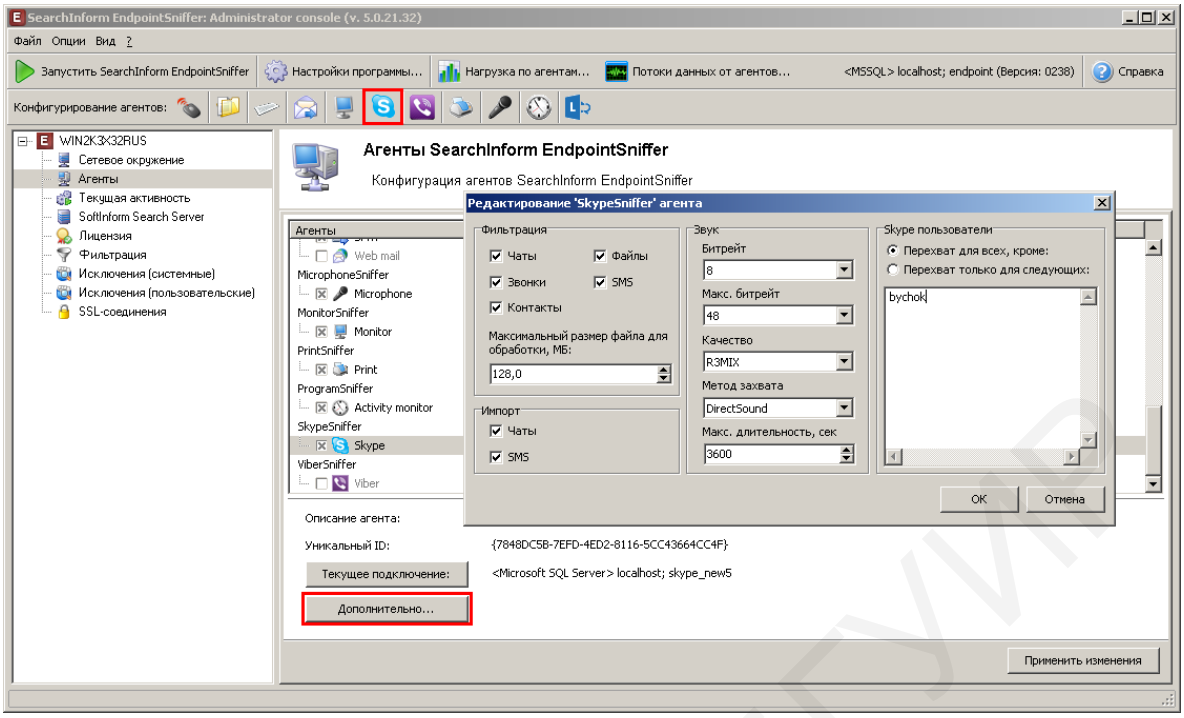


Рис. 2.98. Управление агентом SkypeSniffer

2.4.8. Агент ProgramSniffer

Агент ProgramSniffer предназначен для мониторинга активности запускаемых сотрудником приложений.

Для настройки агента ProgramSniffer (протокол Activity monitor) с подключенной базой нажмите кнопку  на панели «Конфигурирование агентов» либо кнопку «Дополнительно» (рис. 2.99).

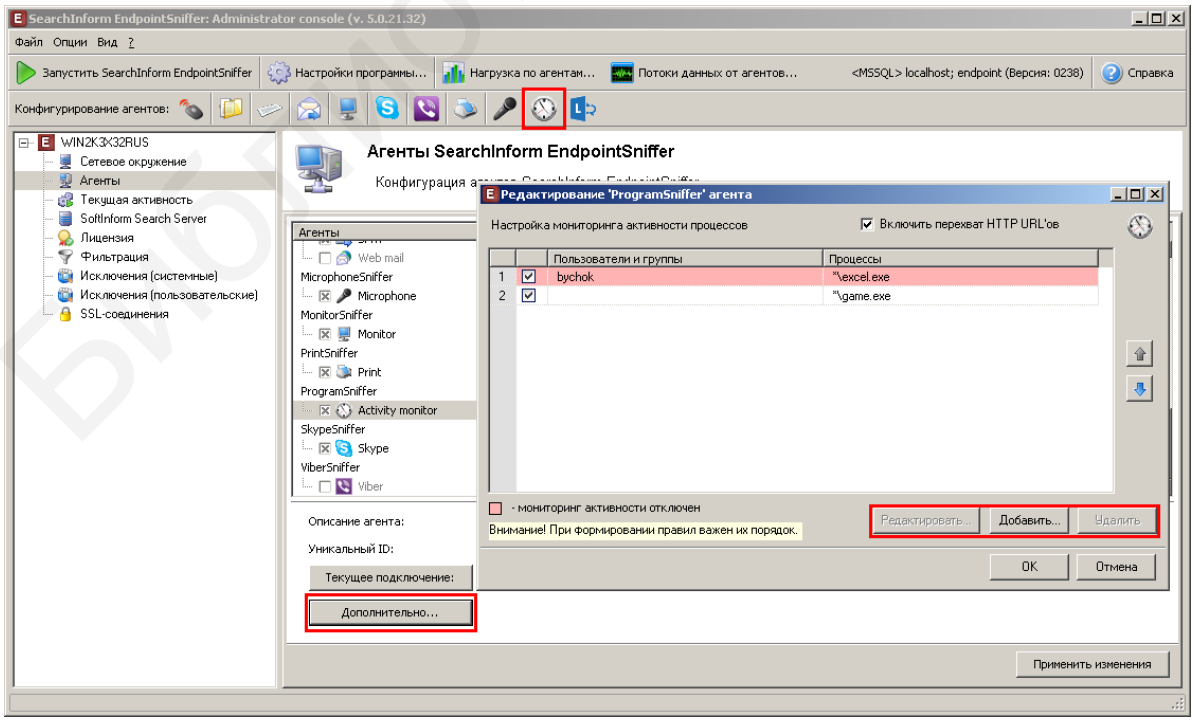


Рис. 2.99. Управление агентом ProgramSniffer

Библиотека БГУИР

В диалоговом окне «Редактирование 'ProgramSniffer' агента» отображается настроенный перечень правил мониторинга активности процессов. Для управления списком используются следующие кнопки:

– «Добавить» – создание нового правила;

– «Редактировать» – изменение имеющегося в списке правила;

– «Удалить» – удаление правила из списка.

Нажмите кнопку «Добавить». Появится диалоговое окно «Добавление правила для ProgramSniffer» (рис. 2.100). Работа со списком пользователей, к которым применяется мониторинг активности либо которые исключаются из мониторинга, производится в левой части окна «Добавление правила для ProgramSniffer», работа со списком процессов, активность которых необходимо фиксировать, – в правой части окна «Добавление правила для ProgramSniffer».

Для фиксирования активности запущенных процессах из столбца «Процессы» должен быть выбран фильтр «Мониторинг активности только для следующих:» (рис. 2.101). Если выбран исключающий фильтр («Мониторинг активности для всех, кроме:»), то для указанных процессов фиксирование активности производиться не будет (оно будет производиться при запуске всех остальных процессов). Введите имя процесса в текстовое поле и нажмите кнопку «Добавить процесс».

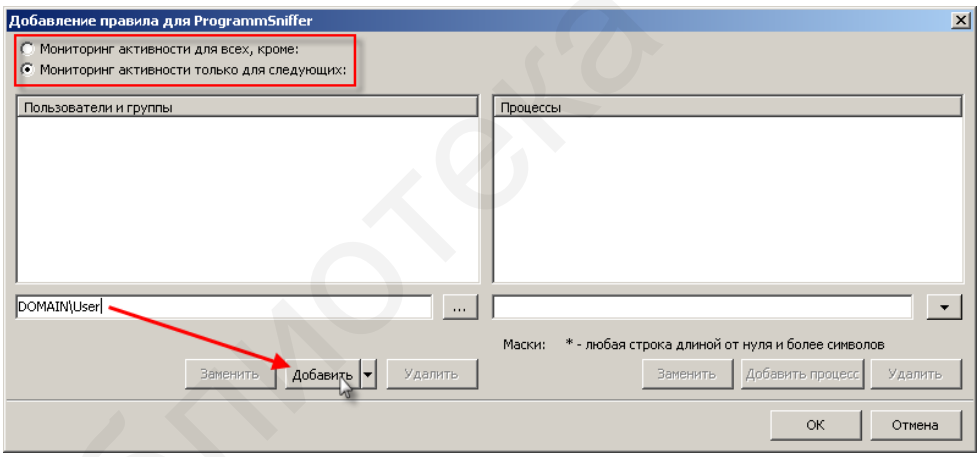


Рис. 2.100. Добавление пользователей

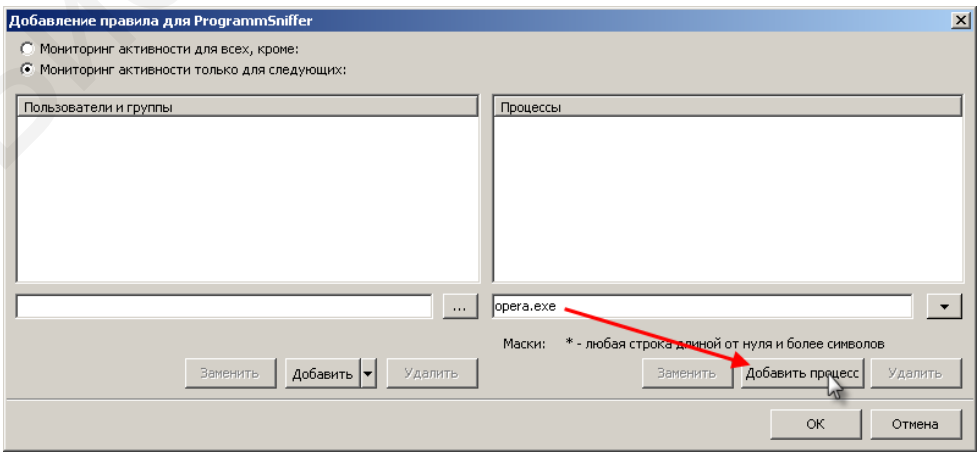


Рис. 2.101. Добавление процессов

Для сохранения настроек в окне редактирования нажмите «OK», а затем нажмите кнопку «Применить изменения» на консоли администрирования.

2.4.9. Агент LyncSniffer

Агент LyncSniffer позволяет перехватывать и анализировать трафик Microsoft Lync: сеансы текстовой и голосовой связи, а также файлы, переданные или полученные при помощи Lync.

Для настройки перехвата данных Lync с подключенной базой выделите протокол Lync и нажмите кнопку  на панели «Конфигурирование агентов» либо кнопку «Дополнительно» (рис. 2.102). В открывшемся окне редактирования агента LyncSniffer произведите необходимые настройки фильтрации каналов данных (чаты, звонки, файлы) и параметров голосовой связи (битрейт, максимальный битрейт, качество и максимальная длительность сеанса связи).

Описание настроек перехвата MS Lync содержится в табл. 2.8.

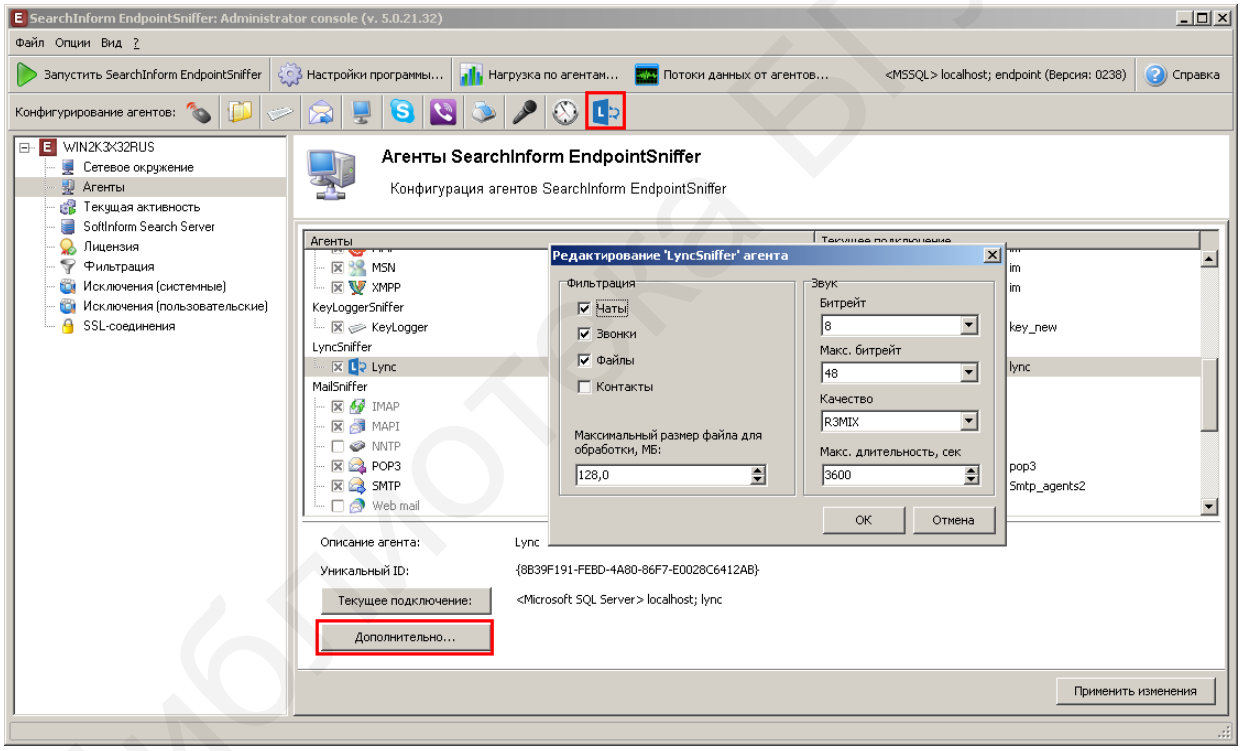


Рис. 2.102. Управление агентом LyncSniffer

Таблица 2.8

Описание настроек агента LyncSniffer

Настройка	Описание
1	**2**
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов
Звонки	Установленный флажок включает перехват сеансов голосовой связи
Файлы	Установленный флажок включает захват файлов, переданных через Lync

Библиотека БГУИР

Окончание табл. 2.8

1	2
Контакты	Установленный флажок включает перехват списков контактов Lync
«Звук»	
Битрейт	Задается битрейт: минимальный – 8 кбит/с, максимально возможный – 320 кбит/с
Макс. битрейт	Задается максимальный битрейт
Качество	Задается качество записываемого сеанса голосовой связи
Макс. длительность, сек	Устанавливается максимальная длительность записываемого сеанса голосовой связи

Для сохранения настроек в окне редактирования агента нажмите «ОК», а затем – кнопку «Применить изменения» на консоли администрирования, чтобы произведенные настройки вступили в силу.

2.4.10. Агент ViberSniffer

Агент ViberSniffer позволяет перехватывать и анализировать трафик Viber: сеансы текстовой и голосовой связи, файлы, переданные при помощи Viber, и списки контактов.

Для настройки параметров перехвата данных Viber выделите протокол Viber и нажмите кнопку  на панели «Конфигурирование агентов» либо кнопку «Дополнительно» (рис. 2.103).

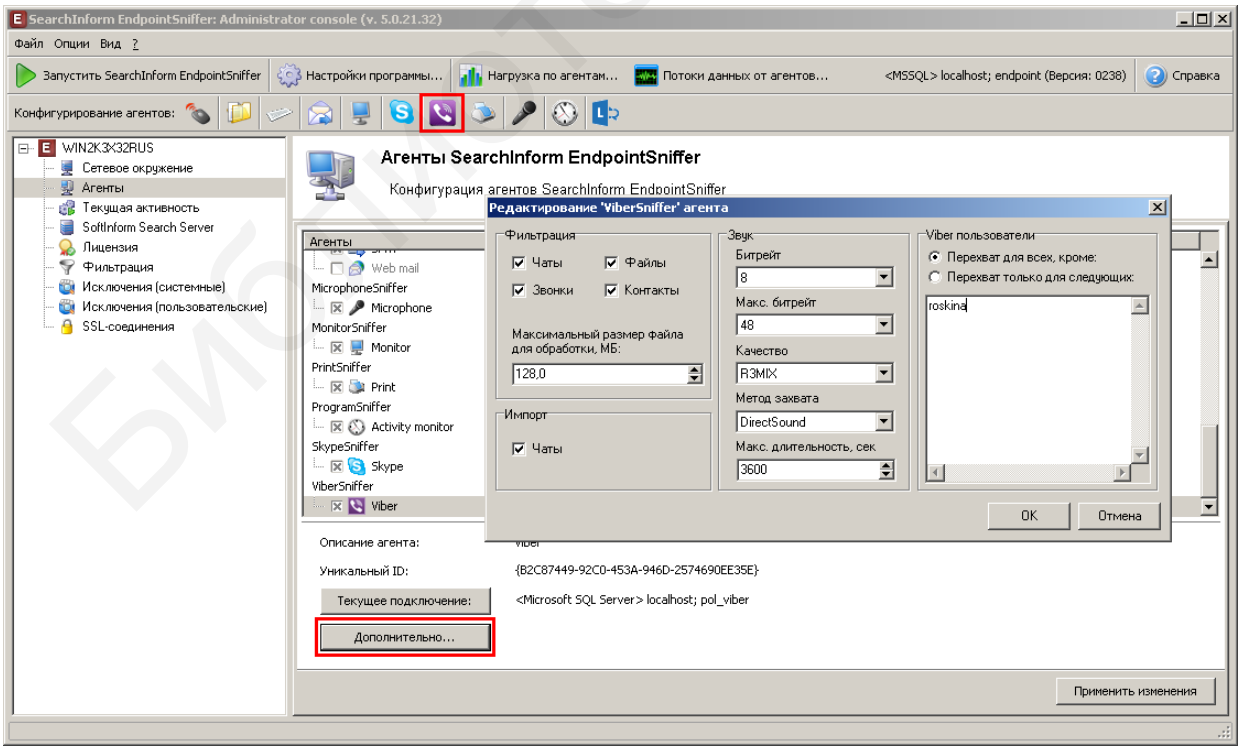


Рис. 2.103. Управление агентом ViberSniffer

Библиотека БГУИР

В открывшемся окне редактирования агента ViberSniffer произведите необходимые настройки фильтрации каналов данных (чаты, звонки, файлы, контакты), импорта, параметров голосовой связи (битрейт, максимальный битрейт, качество и метод захвата, максимальная длительность сеанса связи) и пользователей Viber.

Описание настроек перехвата данных Viber содержится в табл. 2.9.

Таблица 2.9

Описание настроек агента ViberSniffer

Настройка	Описание
«Фильтрация»	
Чаты	Установленный флажок включает перехват чатов
Файлы	Установленный флажок включает захват файлов, переданных через Viber
Звонки	Установленный флажок включает перехват сеансов голосовой связи
Контакты	Установленный флажок включает захват списка контактов из Viber
Максимальный размер файла для обработки, МБ	Задается максимальный размер файла для обработки. Значение по умолчанию – 128 МБ
«Импорт»	
Чаты	Установленный флажок позволяет перехватывать историю сообщений в чатах
«Звук»	
Битрейт	Задается битрейт: минимальный – 8 кбит/с, максимально возможный – 320 кбит/с
Макс. битрейт	Задается максимальный битрейт
Качество	Задается качество записываемого сеанса голосовой связи
Метод захвата	Задается метод захвата звука: DirectSound; Использовать все
Макс. длительность, сек	Устанавливается максимальная длительность записываемого сеанса голосовой связи
«Viber пользователи»	
Перехват для всех, кроме:	Задаются мобильные номера пользователей Viber (через запятую), которые будут исключены из перехвата
Перехват только для следующих:	Задаются мобильные номера (через запятую) только тех пользователей Viber, для которых будет осуществляться перехват

Для сохранения настроек в окне редактирования агента нажмите «ОК», а затем – кнопку «Применить изменения» на консоли администрирования, чтобы произведенные настройки вступили в силу.

Библиотека БГУИР

2.4.11. Агент MobileSniffer

Агент MobileSniffer предназначен для контроля данных, передаваемых с помощью мобильных устройств на базе iOS.

Движение сетевого трафика осуществляется через VPN-сервер, на котором установлен агент с уникальной конфигурацией. Сервер должен иметь внешний IP-адрес, чтобы доступ мобильных устройств к сети через VPN был постоянным.

MobileSniffer включает в себя серверную (агент на VPN-сервере) и клиентскую (агент на мобильном устройстве) части. Агент, установленный на мобильное устройство, перехватывает и передает данные по VPN-каналу. Агент, установленный на VPN-сервер, передает перехваченную информацию на сервер EndpointSniffer.

Для добавления VPN-сервера необходимо на вкладке «Сетевое окружение» нажать кнопку «VPN-сервера», а затем выбрать пункт «Добавить VPN сервер» (рис. 2.104).

Для добавляемого VPN-сервера задаются следующие параметры (рис. 2.105):

– «Имя или IP адрес»;

– «Порт»;

– «Внешний IP адрес»;

– «Интерфейсы»: указываются подсети (в формате <сеть/битовая маска подсети>), для которых будет выполняться перехват.

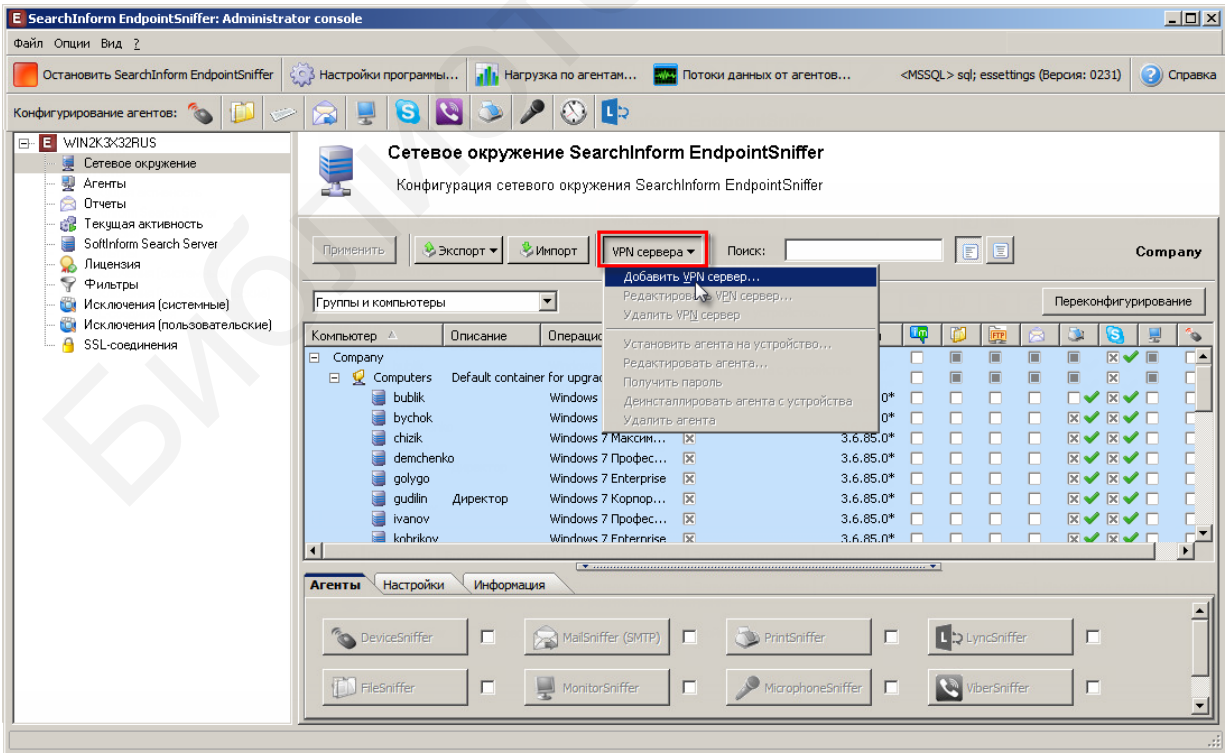


Рис. 2.104. Добавление VPN-сервера

Библиотека БГУИР

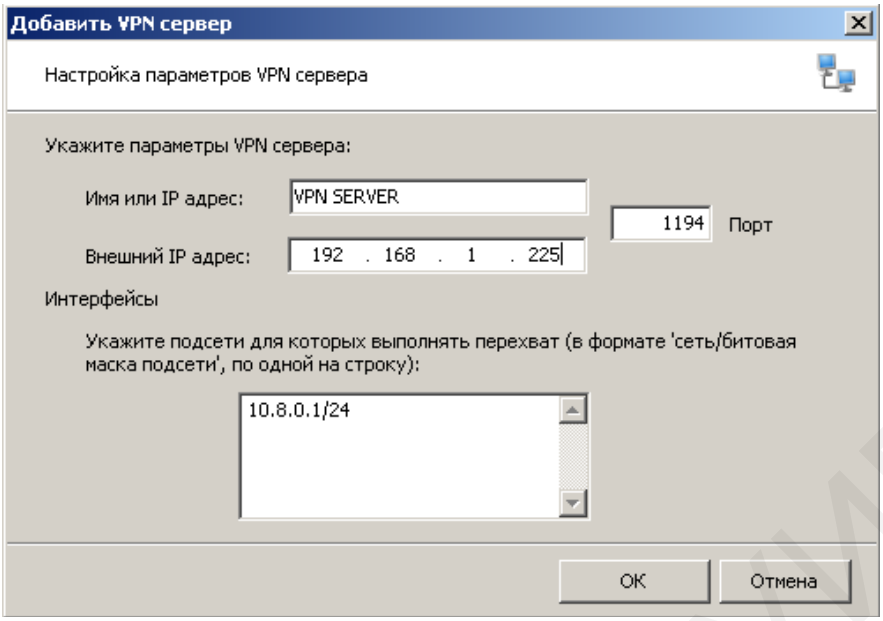


Рис. 2.105. Настройка параметров VPN-сервера

После нажатия «ОК» добавленный VPN-сервер отобразится на вкладке «Сетевое окружение» (должен быть выбран тип отображения «Группы и компьютеры») (рис. 2.106). Для установки агента на VPN-сервер следует установить флажок ☒ в графе «Агент».

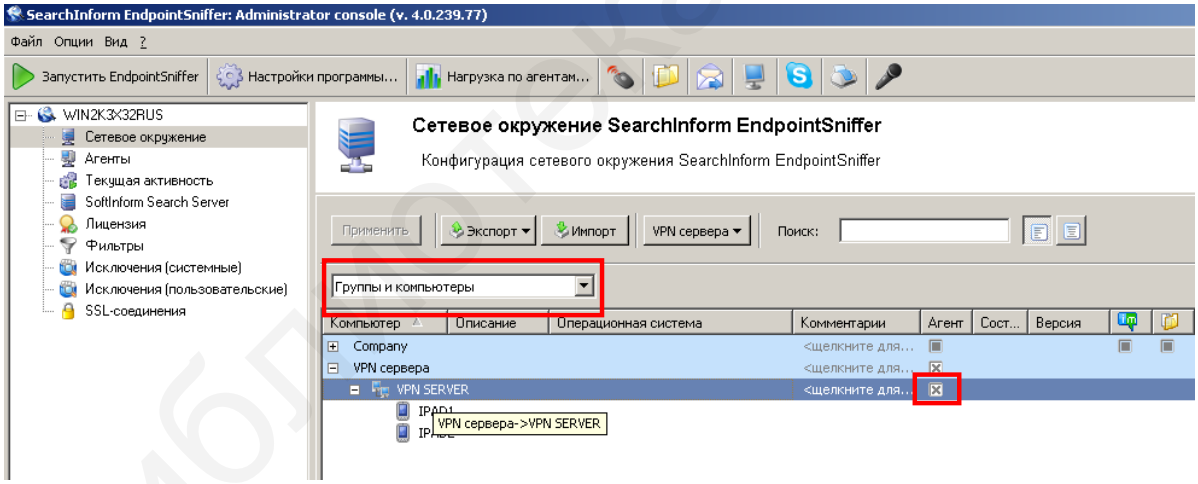


Рис. 2.106. Установка агента на VPN-сервер

Перед установкой агента на устройство должны быть выполнены следующие условия:

– применен Jailbreak;

– установлен OpenSSH;

Для установки агента на мобильное устройство используется кнопка «Установить агента на устройство...» (рис. 2.107).

Библиотека БГУИР

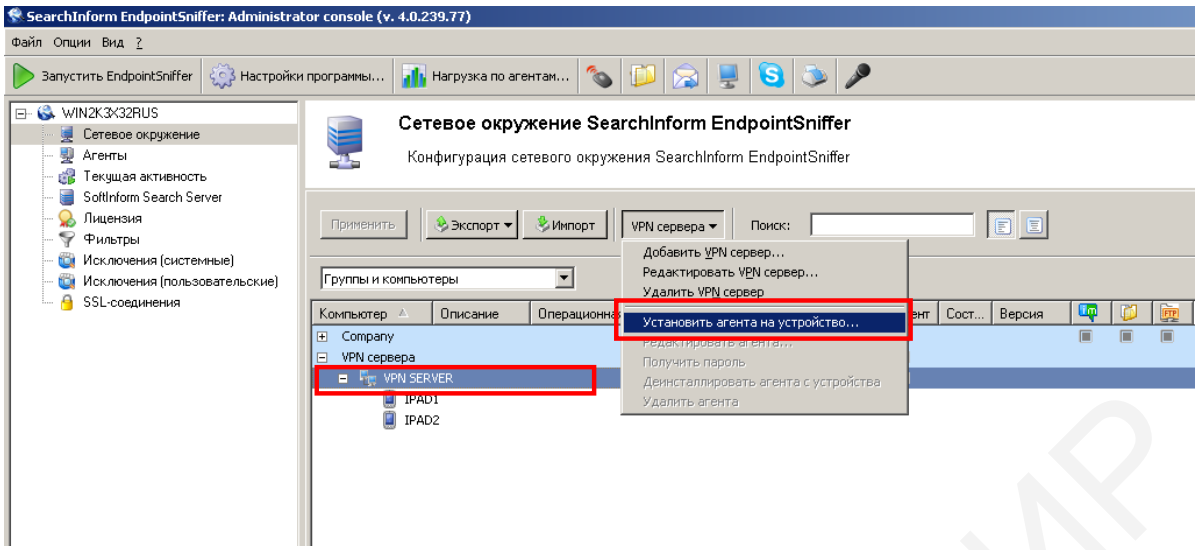


Рис. 2.107. Установка агента на мобильное устройство

При установке агента на устройство задаются следующие параметры (рис. 2.108):

– «ID устройства» – идентификатор устройства, представляющий собой последовательность латинских букв и цифр без пробелов;

– «Пользователь» – имя пользователя;

– «IP адрес»;

– «MAC адрес».

По завершении установки параметров необходимо нажать «ОК». Устройство отобразится в списке VPN-сервера.

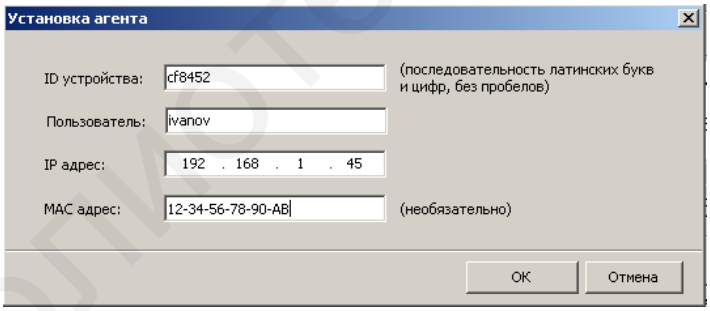


Рис. 2.108. Параметры мобильного устройства, задаваемые при установке агента

Для работы с VPN-серверами используются следующие команды, вызываемые нажатием кнопки на панели или из контекстного меню с помощью правой кнопки мыши (рис. 2.109):

– «Добавить VPN сервер…»;

– «Редактировать VPN сервер…» (для редактирования доступно поле «Интерфейсы»);

– «Удалить VPN сервер».

– «Установить агента на устройство…»;

– «Редактировать агента…» (можно задать/изменить имя пользователя на устройстве);

Библиотека БГУИР

– «Получить пароль…» для пользователя root на мобильном устройстве;

– «Деинсталлировать агента с устройства»;

– «Удалить агента» с VPN-сервера.

Информация о выделенном устройстве отображается в окне в нижней части консоли EndpointSniffer (рис. 2.109): IP-адрес, MAC-адрес, Пользователь, Время установки, Время последней активности агента. При попытке добавления агентов в случае отсутствия лицензий появляется сообщение об ее отсутствии.

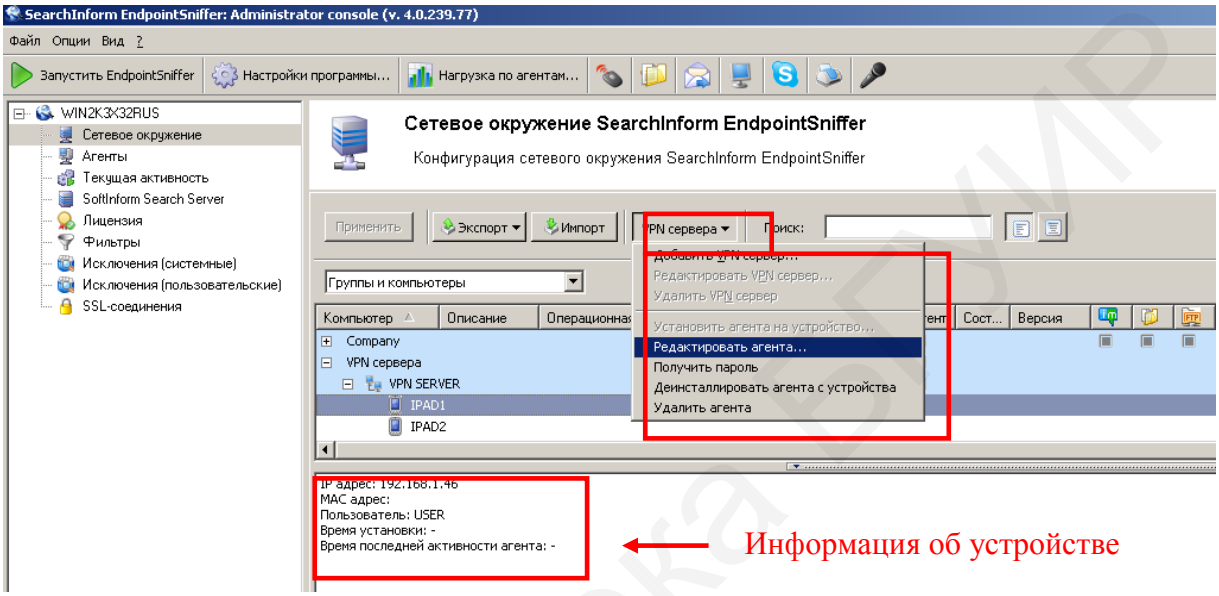


Рис. 2.109. Информация о выделенном мобильном устройстве

Просмотр текущей активности сервера осуществляется при помощи одноименной вкладки консоли администрирования, на которой отображается журнал удачных и неудачных попыток установки агентов на рабочие станции пользователей (рис. 2.110).

Журнал текущего состояния установок агентов включает в себя следующие параметры:

– «Время начала» – дата и время начала первой попытки установить/удалить/обновить агента на рабочей станции;

– «Дата/время» – дата и время начала текущей попытки установить/удалить/обновить агента на рабочую станцию;

– «Компьютер» – имя компьютера, на который устанавливался или был установлен агент;

– «Пользователь» – имя пользователя, инициировавшего активность;

– «Действие» – значок, указывающий на действие, которое производится с агентом;

– «Статус» – значок, отображающий статус сообщения;

– «След. попытка» – дата и время следующей попытки установить/удалить/обновить агента;

Библиотека БГУИР

– «Попыток» – число попыток, предпринятых для установки/удаления/обновления агента;

– «Сообщение» – пояснение о выполнении/невыполнении определенного действия над агентом.

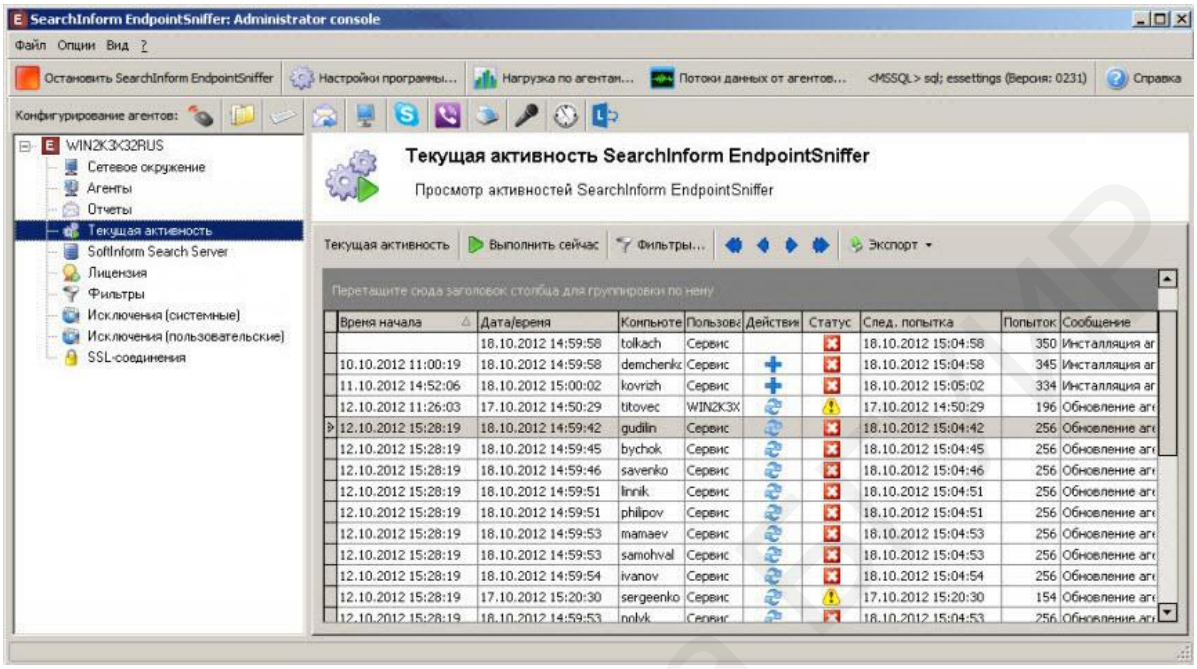


Рис. 2.110. Журнал удачных и неудачных попыток установки агентов на рабочие станции пользователей

Возможные варианты действий, производимых с агентами:

– нет значка – действие не задано;

– ✚ – добавление агента;

– ▬ – удаление агента;

– ⟳ – обновление агента.

Возможные статусы сообщений:

– нет значка – статус не задан;

– ⓘ – сообщение;

– ⚠ – предупреждение;

– ✖ – ошибка.

Расположение колонок относительно друг друга можно менять перетаскиванием заголовков. Сортировка записей по возрастанию-убыванию в выбранной колонке производится щелчком кнопки мыши по заголовку колонки.

Для более удобного просмотра журнала записи можно группировать. Для восстановления расположения столбцов по умолчанию следует воспользоваться командой «Восстановить расположение столбцов» из контекстного меню. Для того чтобы обновить данные о состоянии агентов, необходимо нажать кнопку «Выполнить сейчас».

При большом количестве записей в журнале текущей активности удобно использовать фильтрацию записей (кнопка «Фильтры»). Фильтрацию по выбранному значению можно также производить с помощью контекстного меню, для чего навести указатель мыши на ячейку с требуемым значением (например, со статусом «Предупреждение») и выбрать команду «Добавить значение к фильтру» в контекстном меню. В окне просмотра будут отображены только записи с выбранным значением (рис. 2.111). Для очистки результатов фильтрации в таблице можно воспользоваться командой «Очистить фильтры» контекстного меню.

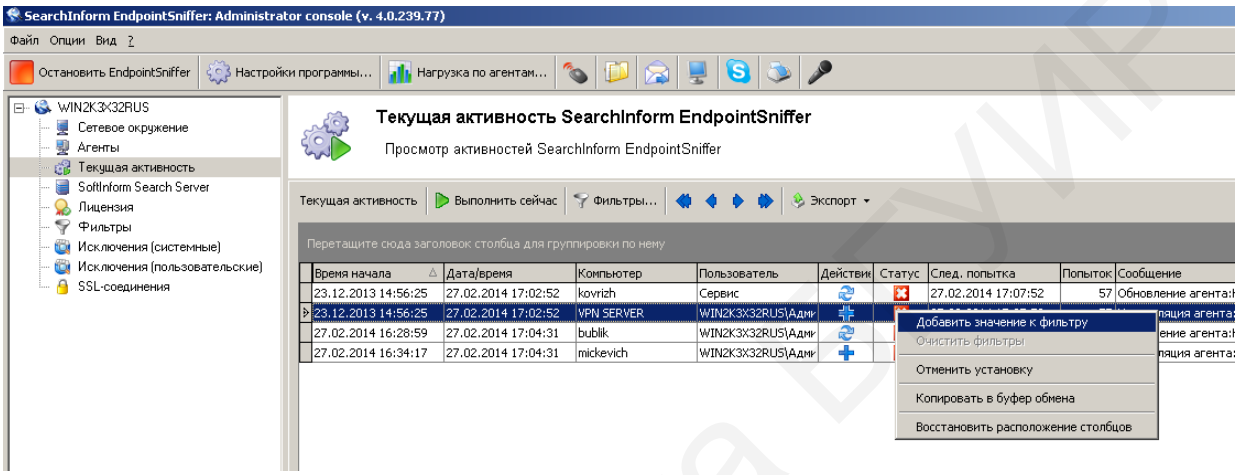


Рис. 2.111. Фильтрация по выбранному значению
при помощи контекстного меню

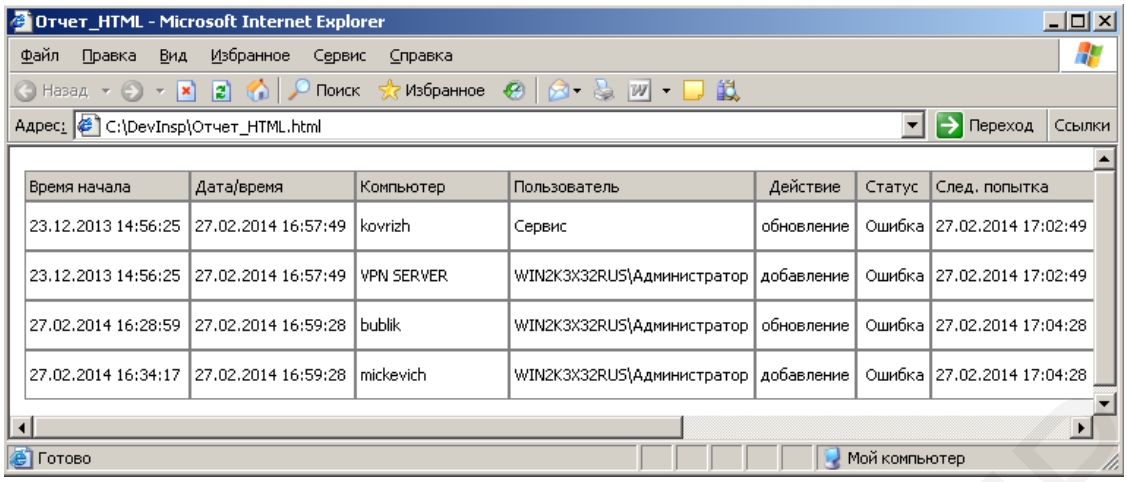
Навигацию по записям удобно выполнять с помощью направляющих стрелок. Для отмены установки агентов на рабочие станции необходимо выделить требуемые компьютеры и воспользоваться командой «Отменить установку» из контекстного меню. Процесс установки прервется, и выделенные записи будут удалены из журнала.

Для множественного выбора записей в журнале текущего состояния используются добавочные клавиши CTRL и SHIFT.

Действие команды «Копировать в буфер обмена» из контекстного меню распространяется только на ячейку, на которую наведен указатель мыши. Данные в других ячейках выделенной области скопированы не будут.

При помощи кнопки «Экспорт» журнал текущего состояния установок агентов можно экспортировать в файлы форматов HTML, XLS, TXT и сохранять в заданное место на диске. Образец HTML-отчета представлен на рис. 2.112.

Библиотека БГУИР



Время начала	Дата/время	Компьютер	Пользователь	Действие	Статус	След. попытка
23.12.2013 14:56:25	27.02.2014 16:57:49	kovrizh	Сервис	обновление	Ошибка	27.02.2014 17:02:49
23.12.2013 14:56:25	27.02.2014 16:57:49	VPN SERVER	WIN2K3X32RUS\Администратор	добавление	Ошибка	27.02.2014 17:02:49
27.02.2014 16:28:59	27.02.2014 16:59:28	bublik	WIN2K3X32RUS\Администратор	обновление	Ошибка	27.02.2014 17:04:28
27.02.2014 16:34:17	27.02.2014 16:59:28	mickevich	WIN2K3X32RUS\Администратор	добавление	Ошибка	27.02.2014 17:04:28

Рис. 2.112. Образец HTML-отчета о текущем состоянии установок агентов

Работа с индексами. Как уже было отмечено, поисковые индексы необходимы для анализа перехваченных данных и поиска по ним. Для осуществления операций с индексами локально или в сети должен быть установлен сервер SoftInform Search. Взаимодействие серверов EndpointSniffer и SoftInform Search осуществляется через порт 25012. С помощью консоли администратора SearchInform EndpointSniffer можно создавать только индексы протоколов, запись которых в базу данных производится самим сервером. Исключение – продукты FileSniffer, MonitorSniffer, MicrophoneSniffer и KeyloggerSniffer, которые не используют индексы. Список протоколов, индексы которых можно создать в консоли, содержится в табл. 2.10.

Таблица 2.10

Список протоколов, индексы которых можно создать в консоли администратора SearchInform EndpointSniffer

Данные	**Продукт**	**Протоколы (обозначение в консоли)**
Файлы облачных хранилищ данных	CloudSniffer	Cloud
Файлы, переданные на внешние устройства	DeviceSniffer	Device
Файлы, полученные или переданные по FTP	FTPSniffer	FTP
Сообщения и файлы, отправленные при помощи браузера	HTTPSniffer	HTTP
Мгновенные сообщения, файлы. Текстовые сообщения, голосовые звонки и файлы Microsoft Lync. Текстовые сообщения, файлы, голосовые звонки, контакты Viber Desktop	IMSniffer	Gadu-Gadu, ICQ, MMP, MSN, XMPP, HTTPIM, Lync, Viber
Сообщения и вложения электронной почты	MailSniffer	SMTP, POP3, NNTP, IMAP, MAPI
Данные, отправленные на печать	PrintSniffer	Print
Skype (текстовые сообщения и SMS, файлы, голосовые звонки)	SkypeSniffer	Skype

Библиотека БГУИР

Стандартные операции с индексами, которые могут быть осуществлены в консоли EndpointSniffer:

– создание индекса;

– подключение индекса;

– настройка расписания обновления индекса;

– обновление индекса вручную;

– очистка и удаление индекса.

Содержание стандартных операций с индексами было рассмотрено в подразд. 2.1 и 2.2.

Настройка фильтрации. Применительно к платформе SearchInform EndpointSniffer под фильтрацией понимается ограничение перехвата документов по следующим атрибутам документов: пользователь домена, IP- и MAC-адреса. Основным предназначением данной функции является исключение из мониторинга отдельных пользователей, например, руководства и ответственных работников организации. Могут быть и иные причины, требующие ограничения перехвата. Возможная альтернатива фильтрации перехваченных данных – удаление агентов с тех рабочих станций, которые не нужно подвергать мониторингу. Тем не менее фильтрация необходима, если есть рабочие станции или терминальные серверы, которыми могут пользоваться и те, кого нужно подвергать мониторингу, и те, кого нужно исключить из мониторинга.

Фильтрация по пользователям и группам происходит на агенте для фильтров (как глобальных, так и фильтров по протоколам), а также для протоколов SMTP и POP3 почтовой фильтрации. Логические стадии фильтрации на агентах следующие.

1. Установленные на рабочие станции агенты производят теневое копирование перехваченной информации и сверяют атрибуты каждого полученного пакета данных по имеющимся фильтрам. При настройках «по умолчанию» (если фильтры не были установлены), фильтрация не осуществляется и все пакеты данных без исключения передаются на сервер. Если фильтры были настроены, то часть пакетов может отсеиваться в соответствии с настройками.

2. Сервер управления записывает переданные пакеты данных в базы данных.

Остальная фильтрация происходит на сервере управления. Логика фильтрации выглядит следующим образом.

1. Вне зависимости от параметров фильтрации установленные на рабочие станции агенты производят теневое копирование перехваченной информации и передают ее на сервер управления.

2. Сервер управления сверяет атрибуты каждого полученного пакета данных по имеющимся фильтрам. При настройках «по умолчанию» (если фильтры не были установлены) фильтрация не осуществляется и все пакеты данных без исключения помещаются в базы данных. Если фильтры были настроены, то часть пакетов может отсеиваться, не будучи записанной в базу данных.

Сервер управления может фильтровать трафик как по всем, так и по отдельным каналам передачи данных. Фильтрация может произво-

Библиотека БГУИР

диться по трем атрибутам пакетов: имени локального пользователя, IP-адресу локального или удаленного пользователя и MAC-адресу локального пользователя. Настройка фильтрации осуществляется на вкладке «Фильтры» в левой части консоли администрирования (рис. 2.113). При этом настройка общих фильтров для всех поддерживаемых каналов передачи производится на вкладке «Глобальные фильтры», а настройка фильтров по отдельным протоколам – на вкладке «Фильтры по протоколам». Для включения фильтрации необходимо установить флажок в строке «Включить фильтрацию», для сохранения произведенных настроек фильтрации – воспользоваться кнопкой «Применить изменения».

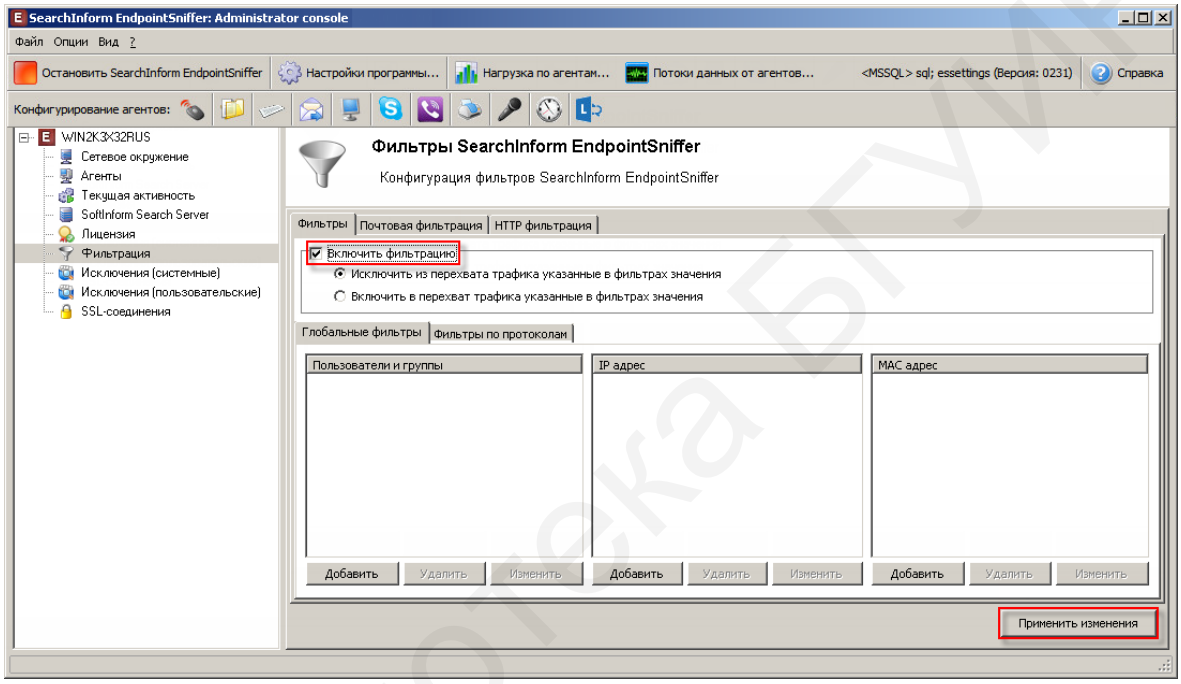


Рис. 2.113. Настройка фильтрации в консоли администрирования SearchInform EndpointSniffer

Общие правила работы фильтров:

– если опция фильтрации включена, но список фильтров пуст, перехват будет осуществляться без ограничений по адресам;

– чтобы пакет данных попал под правило («запретить» или «разрешить» перехват), достаточно совпадения по одному атрибуту;

– одновременно можно использовать или только запрещающие фильтры, или только разрешающие;

– при использовании запрещающих фильтров в базу данных будут передаваться все перехваченные пакеты за исключением совпадений по фильтрам; для запрещающей фильтрации должна быть включена опция «Исключить из перехвата трафика...»;

– при использовании разрешающих фильтров в базу данных будут переданы все перехваченные пакеты, совпадающие с фильтрами; для разрешающей фильтрации должна быть включена опция «Включить в перехват трафика...».

Библиотека БГУИР

При настройке фильтра по пользователям домена можно вручную ввести одного или нескольких пользователей. Ввод нескольких пользователей производится через запятую (рис. 2.114). Также можно воспользоваться кнопкой  и получить список пользователей из одного из трех источников: DataCenter, Active Directory, NetBIOS. Особенности процедуры получения списка пользователей были рассмотрены в подразд. 2.2.

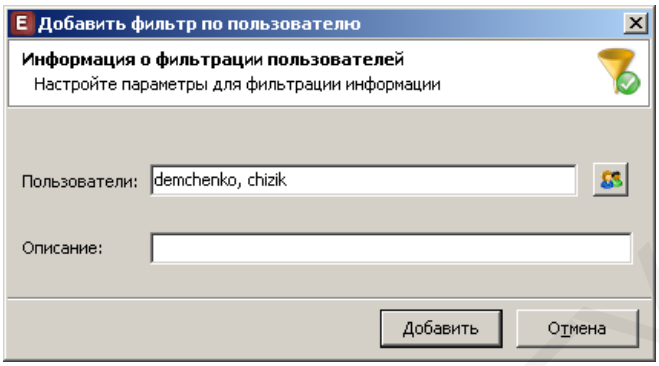


Рис. 2.114. Настройка фильтра по пользователям домена

При настройке фильтров по IP-адресам можно использовать отдельные IP-адреса, диапазоны IP-адресов и сетевые маски (рис. 2.115). В качестве фильтров можно применять отдельные MAC-адреса (рис. 2.116).

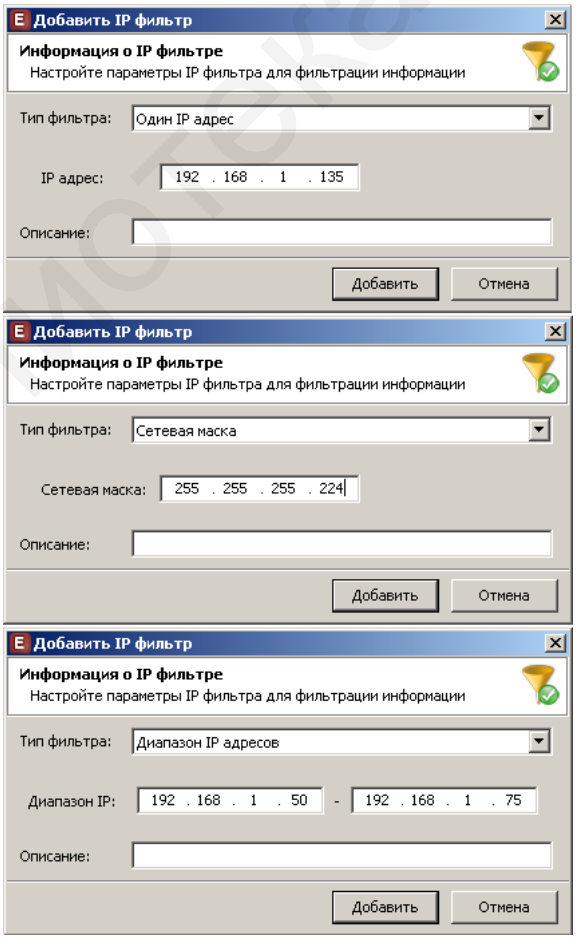


Рис. 2.115. Настройка фильтров по IP-адресам

Библиотека БГУИР

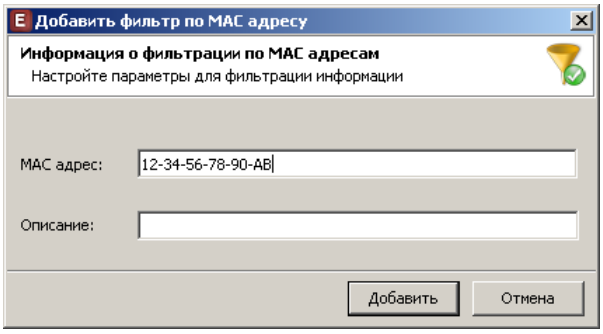


Рис. 2.116. Настройка фильтра по MAC-адресу

Настройка глобальных фильтров. Глобальные фильтры применяются для всех протоколов и продуктов. При этом должна быть включена фильтрация и выбран запрещающий или разрешающий режим фильтрации.

Настройка общих фильтров производится на вкладке «Глобальные фильтры». Для добавления фильтра следует воспользоваться одной из трех имеющихся кнопок «Добавить» и ввести атрибуты фильтрации: Имя пользователя домена, IP-адрес и MAC-адрес. Добавленные фильтры будут отображены в консоли EndpointSniffer (рис. 2.117).

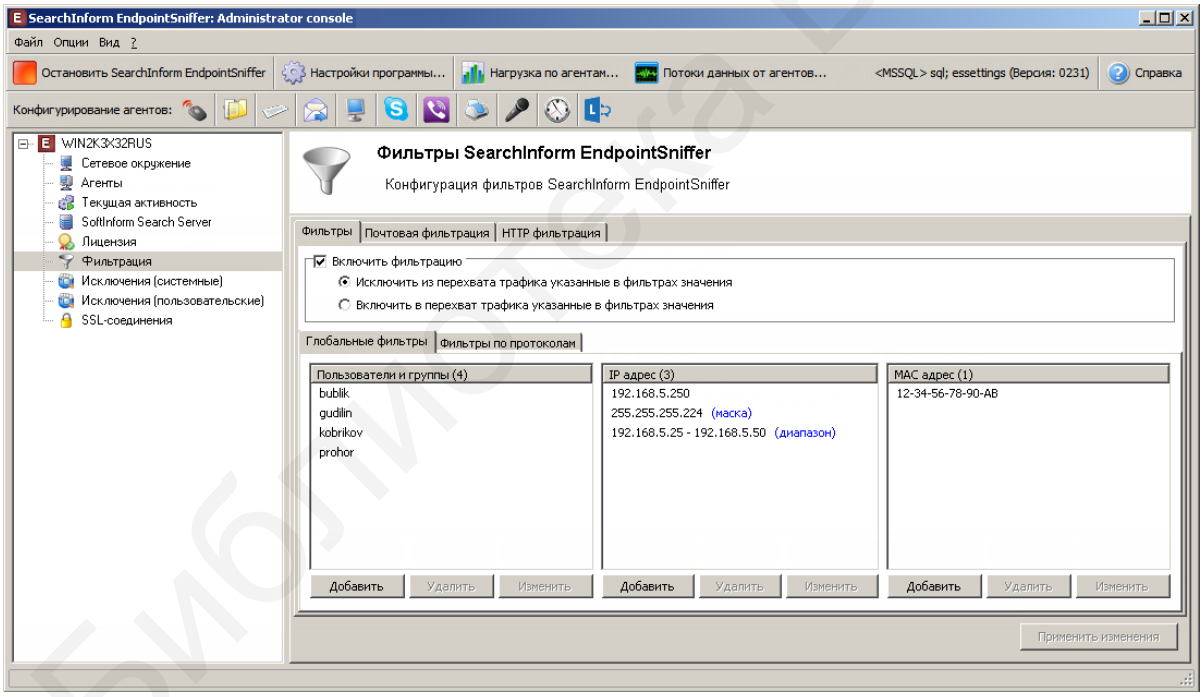


Рис. 2.117. Настройка глобальных фильтров

Для удаления и изменения настроек фильтров используются кнопки «Удалить» и «Изменить». Помимо кнопки «Удалить» для очистки фильтров можно выбрать команду «Очистить» из контекстного меню, вызываемого при помощи щелчка правой кнопкой мыши. Данное действие распространяется только на ту колонку (Имя пользователя, IP-адрес, MAC-адрес), в пределах которой находится указатель мыши. При этом независимо от количества выделенных позиций команда «Очистить» удаляет все имеющиеся в колонке данные.

Библиотека БГУИР

Фильтры по протоколам применяются для выбранных протоколов. При этом должна быть включена фильтрация и выбран запрещающий или разрешающий режим фильтрации.

Настройка частных фильтров производится на вкладке «Фильтры по протоколам». Для добавления фильтра необходимо выбрать имя агента и затем воспользоваться одной из трех кнопок «Добавить», после чего ввести атрибуты фильтрации: Имя пользователя домена, IP-адрес и MAC-адрес. Добавленные фильтры будут отображены в консоли EndpointSniffer (рис. 2.118).

На вкладке «Фильтры по протоколам» отображаются и глобальные фильтры для всех агентов, и фильтры по протоколам для отдельных агентов. Слева от глобальных фильтров располагаются чекбоксы .

Для удаления и изменения настроек фильтров используются кнопки «Удалить» и «Изменить». Для очистки фильтров также можно выбрать команду «Очистить» из контекстного меню, вызываемого при помощи щелчка правой кнопкой мыши. Данное действие распространяется только на ту колонку (Имя пользователя, IP-адрес, MAC-адрес), в пределах которой находится указатель мыши. При этом независимо от количества выделенных позиций команда «Очистить» удаляет все имеющиеся в колонке данные.

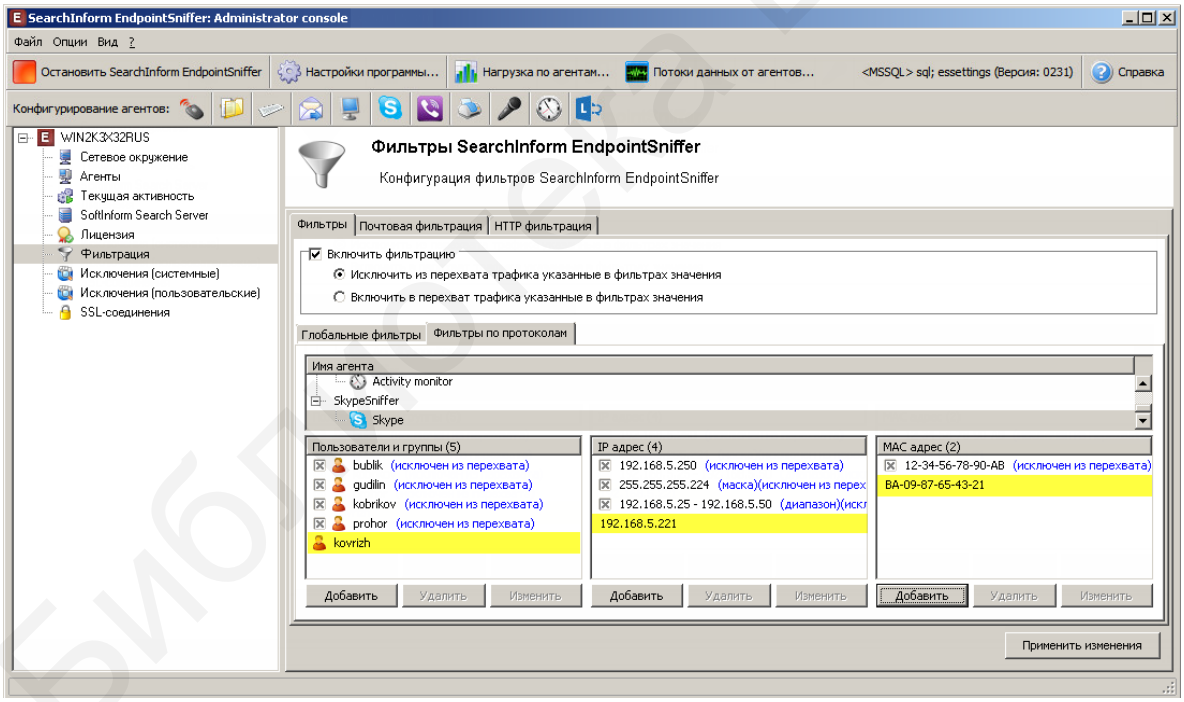


Рис. 2.118. Настройка фильтров по протоколам

Управление фильтрами. Пользователь может загрузить сохраненную ранее конфигурацию фильтров из заданной директории. Для загрузки конфигурации фильтров следует выбрать команду «Загрузить конфигурацию...» из контекстного меню, вызываемого при помощи щелчка правой кнопкой мыши. Далее необходимо сделать выбор в отношении сохранения текущих настроек фильтров перед загрузкой новой конфигурации, после чего указать

Библиотека ВГУИР

путь к загружаемому файлу XML. После нажатия кнопки «Открыть» импортированная конфигурация будет отображена в консоли EndpointSniffer. Для вступления настроек фильтрации в силу необходимо нажать кнопку «Применить изменения». В свою очередь, настроенная конфигурация может быть сохранена в файл формата XML. Для этого используется команда «Сохранить конфигурацию» в контекстном меню. В процессе выполнения указанной операции необходимо задать имя файла XML, который будет хранить конфигурацию фильтров, и определить директорию, где этот файл будет храниться.

Отдельный фильтр или группа фильтров могут быть импортированы в приложение из указанного пользователем файла (формат TXT). Чтобы выделить все фильтры в колонке, следует выбрать команду «Выделить / снять выделение для всех» из контекстного меню, вызываемого при помощи щелчка правой кнопкой мыши. Отмена выделения всех позиций производится повторным щелчком по той же команде. Для импорта фильтров необходимо выбрать команду «Импортировать...» из контекстного меню, указать путь к загружаемому файлу TXT. После нажатия кнопки «Открыть» импортированный фильтр будет отображен в консоли EndpointSniffer. Для вступления настроек фильтрации в силу необходимо нажать кнопку «Применить изменения».

Точно так же фильтр или группа фильтров могут быть экспортированы из приложения в указанный пользователем файл. Для этого используется команда «Экспортировать...» в контекстном меню. В процессе выполнения указанной операции необходимо задать имя файла, который будет хранить данные о фильтре, и определить директорию, где этот файл будет храниться.

Почтовая фильтрация работает для сообщений, передаваемых по почтовым протоколам. Для настройки выделите в левой части окна узел «Фильтрация» и откройте вкладку «Почтовая фильтрация». Установите флажок в строке «Включить фильтрацию» и нажмите кнопку «Добавить» (рис. 2.119).

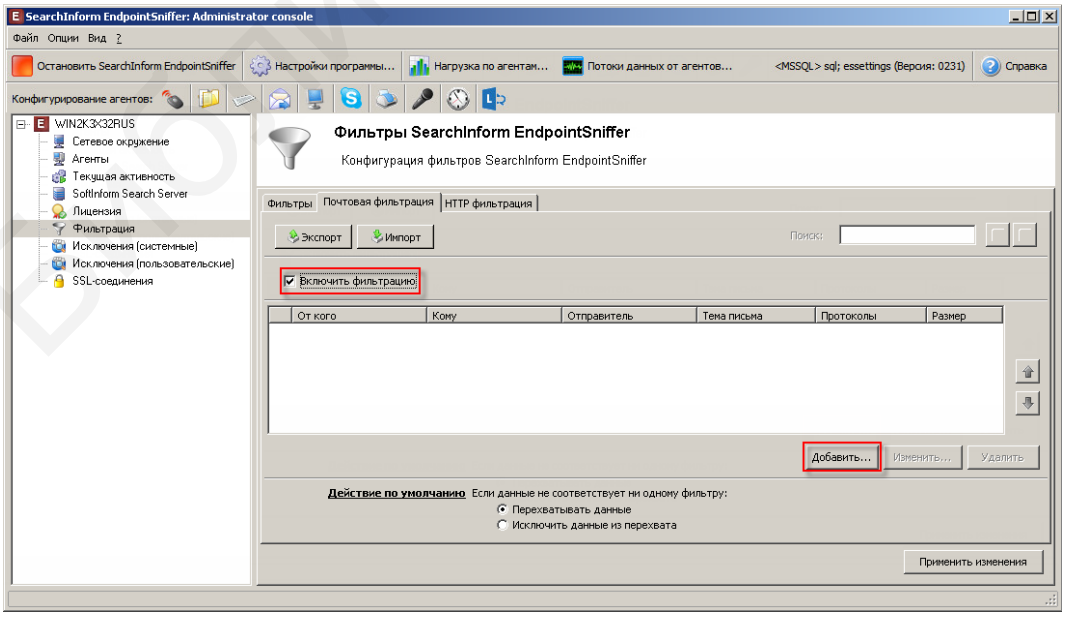


Рис. 2.119. Включение почтовой фильтрации

Библиотека БГУИР

В открывшемся окне (рис. 2.120) задайте параметры фильтра.

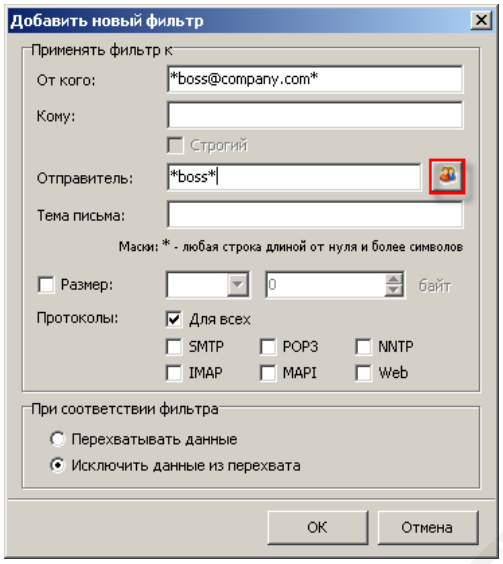


Рис. 2.120. Настройка фильтра

Рекомендуется, чтобы обрабатываемые доменные имена и адреса получателей/отправителей сообщений начинались и заканчивались маской с символом «*», подразумевающим любое количество и сочетание символов.

Также можно нажать кнопку  и получить список пользователей, применить один из трех источников: DataCenter, Active Directory, NetBIOS.

Фильтры имеют приоритет и применяются последовательно в том порядке, в котором они заданы. Чем выше расположен фильтр, тем раньше он сработает.

Установите действие по умолчанию, если письмо не будет соответствовать ни одному из фильтров: либо «Перехватывать письмо», либо «Исключить письмо из перехвата».

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

HTTP-фильтрация работает для GET/POST-запросов, передаваемых по протоколу HTTP.

Для настройки фильтрации по протоколу HTTP выделите в левой части окна узел «Фильтрация» и откройте вкладку «HTTP фильтрация». Установите флажок в строке «Включить фильтрацию» и нажмите кнопку «Добавить» (рис. 2.121).

Библиотека БГУИР

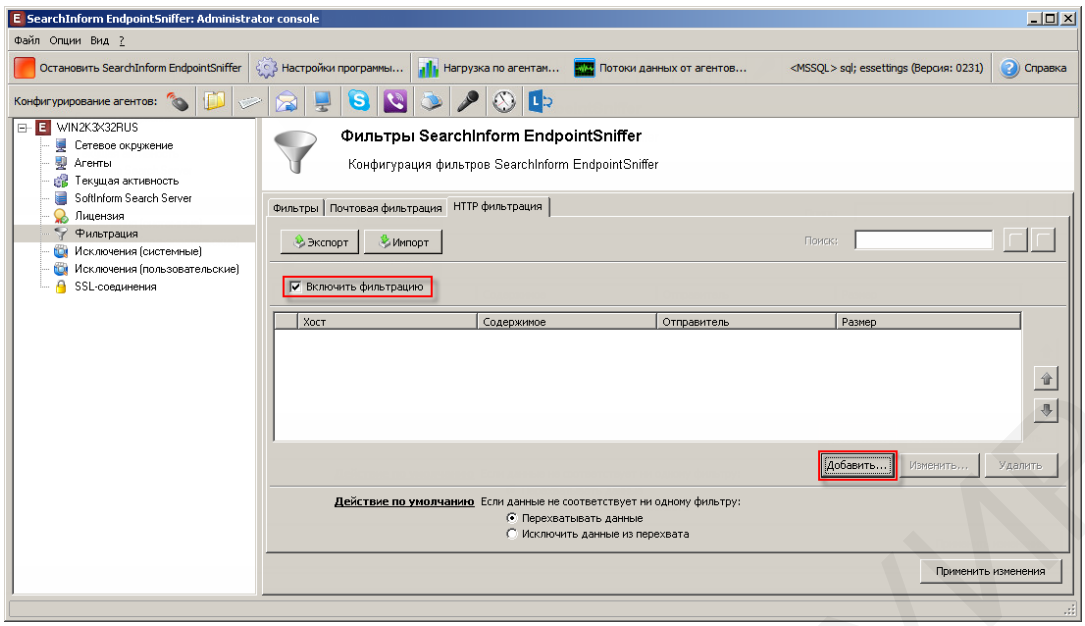


Рис. 2.121. HTTP-фильтрация

Укажите значения атрибутов документа (рис. 2.122), к которым будет применен фильтр, предварительно установив напротив него флажок:

– «Хост» – адрес ресурса в сети;

– «Содержимое» – данные POST/GET-запроса;

– «Отправитель» – полное доменное имя отправителя запроса.

– «Размер» – размер запроса.

В имени хоста и отправителя допускается использование метасимвола «*», заменяющего необходимое количество символов (от нуля и более).

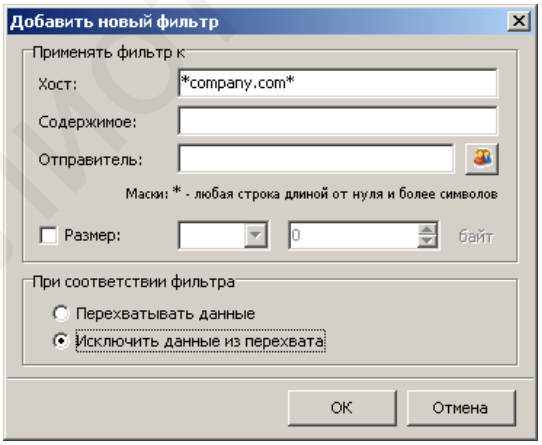


Рис. 2.124. Настройка фильтра

Установите действие по умолчанию, если перехваченные данные не будут соответствовать ни одному из фильтров: либо «Перехватывать данные», либо «Исключить данные из перехвата».

Фильтры могут быть экспортированы в указанный пользователем файл в формате XML. В свою очередь, сохраненный список фильтров может быть импортирован в приложение из указанного пользователем файла. Для управления используйте кнопки «Экспорт» и «Импорт».

Настройка исключений применяется для того, чтобы работа агентов EndpointSniffer не препятствовала выполнению стандартных системных процессов, а также не распространялась на некоторые доверенные программы. Стандартные системные процессы должны быть исключены из обработки агентами. Исключения такого рода процессов не могут редактироваться, они добавляются с помощью импортирования. Также возможны случаи, когда при наличии запущенных агентов EndpointSniffer пользовательские программные приложения (например, антивирусное ПО, банковские клиенты, компоненты сторонних DLP-систем) перестают функционировать. Подобным образом могут вести себя и различные системы электронного документооборота при взаимодействии с агентами EndpointSniffer.

При обнаружении некорректной работы приложений в системе с установленным агентом EndpointSniffer конфликтующие пользовательские приложения могут быть внесены в список исключений EndpointSniffer. Для этого используется функция исключения процессов.

В свою очередь, процессы EndpointSniffer могут быть добавлены в список исключений конфликтующих приложений. При использовании EndpointSniffer совместно с антивирусными программами настройка взаимных исключений является обязательной!

В список исключений могут быть также занесены хосты, располагающие встроенной защитой от мониторинга передаваемых данных. Для этой цели предусмотрена функция исключения хостов. Для постоянного мониторинга хостов с защищенным SSL-соединением предназначена вкладка «Хосты (мониторинг SSL)». В отношении списков исключений могут применяться операции импорта и экспорта. Настройка и управление исключениями производятся на вкладках «Исключения (системные)» (рис. 2.123) и «Исключения (пользовательские)» (рис. 2.124).

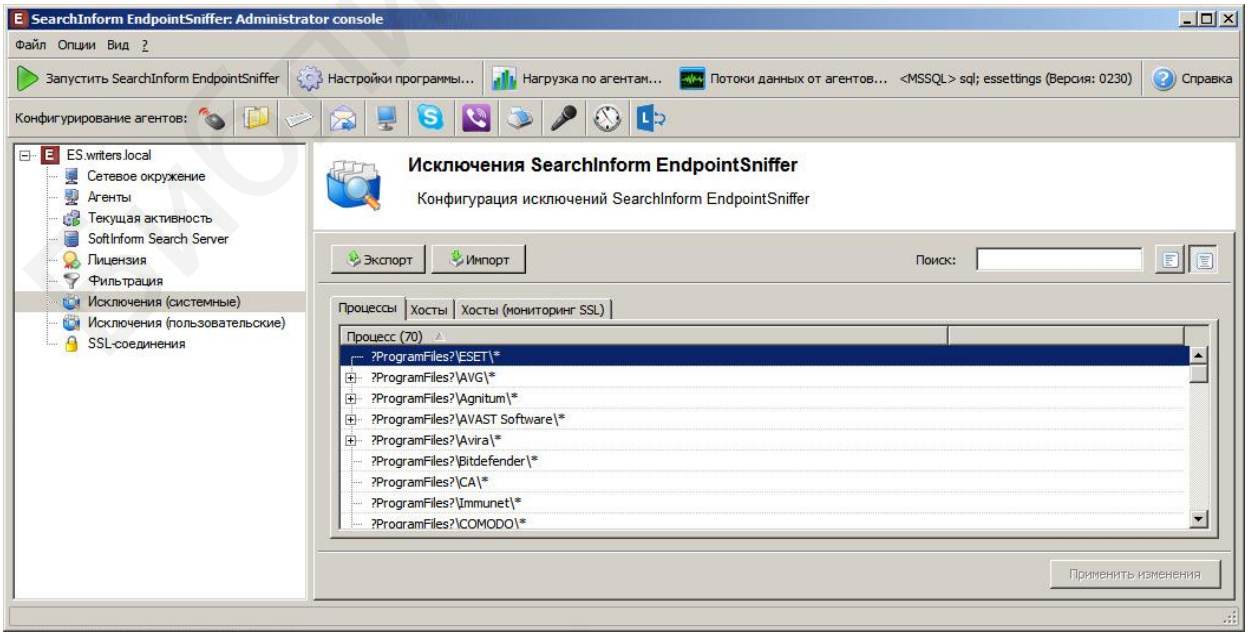


Рис. 2.123. Настройка исключений (системных)

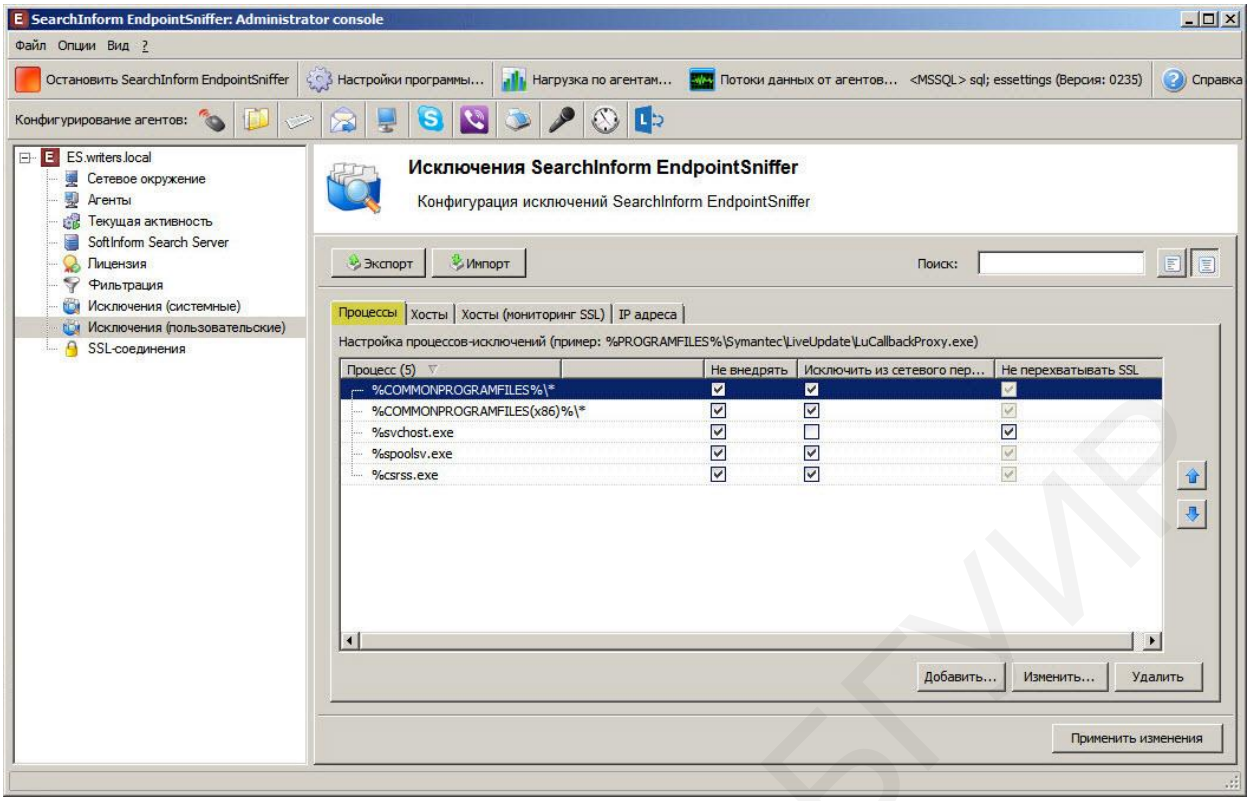


Рис. 2.124. Настройка исключений (пользовательских)

Узел настроек «SSL-соединения» предназначен для просмотра журнала соединений SSL. Перехват трафика, передаваемого по защищенному SSL-соединению, система производит путем подмены оригинального сертификата на собственный. Если в результате отклика на данное действие связь прерывается либо система получает уведомление об ошибке, сервер EndpointSniffer возвращает соединению «родной» сертификат, а программу (хост) заносит в список исключений на агентах.

Консоль администрирования EndpointSniffer позволяет просматривать журнал SSL-соединений, во время установления которых произошли ошибки. Просмотр журнала осуществляется на вкладке «SSL-соединения» консоли администрирования EndpointSniffer (рис. 2.125).

Для актуализации записей журнала служит кнопка «Обновить», навигацию по записям можно выполнять с помощью направляющих стрелок. Для более удобного просмотра журнала записи можно группировать. Порядок группировки записей идентичен тому, что используется в журнале текущей активности. Для восстановления исходного расположения столбцов следует применить команду «Восстановить расположение столбцов» из контекстного меню.

По умолчанию исключения на агентах добавляются автоматически. В случае необходимости пополнять перечень исключений на агентах вручную (используя файл конфигурации) следует снять флажок в строке «Автоматически добавлять исключения на агентах».

Автоматически добавленные локальные исключения на агентах отображаются в журнале SSL-соединений зеленым фоном.

Библиотека БГУИР

Допустимое число неудачных подключений (по умолчанию – 1), после которого соединение будет добавлено в исключения на агентах, можно изменять. Журнал SSL-соединений позволяет быстро добавить процессы и хосты неудачных соединений в пользовательские исключения.

Для добавления процесса по выбранному соединению в исключения необходимо воспользоваться командой «Добавить процессы в исключения» из контекстного меню. Процесс будет добавлен в список пользовательских исключений (вкладка «Процессы»).

Для добавления хоста по выбранному соединению в исключения необходимо воспользоваться командой «Добавить хосты в исключения» из контекстного меню. Хост будет добавлен в список пользовательских исключений (вкладка «Хосты»).

Для удаления выбранного соединения из исключений на агентах служит команда «Удалить из исключений на агентах» из контекстного меню. Система будет пытаться перехватить трафик такого соединения.

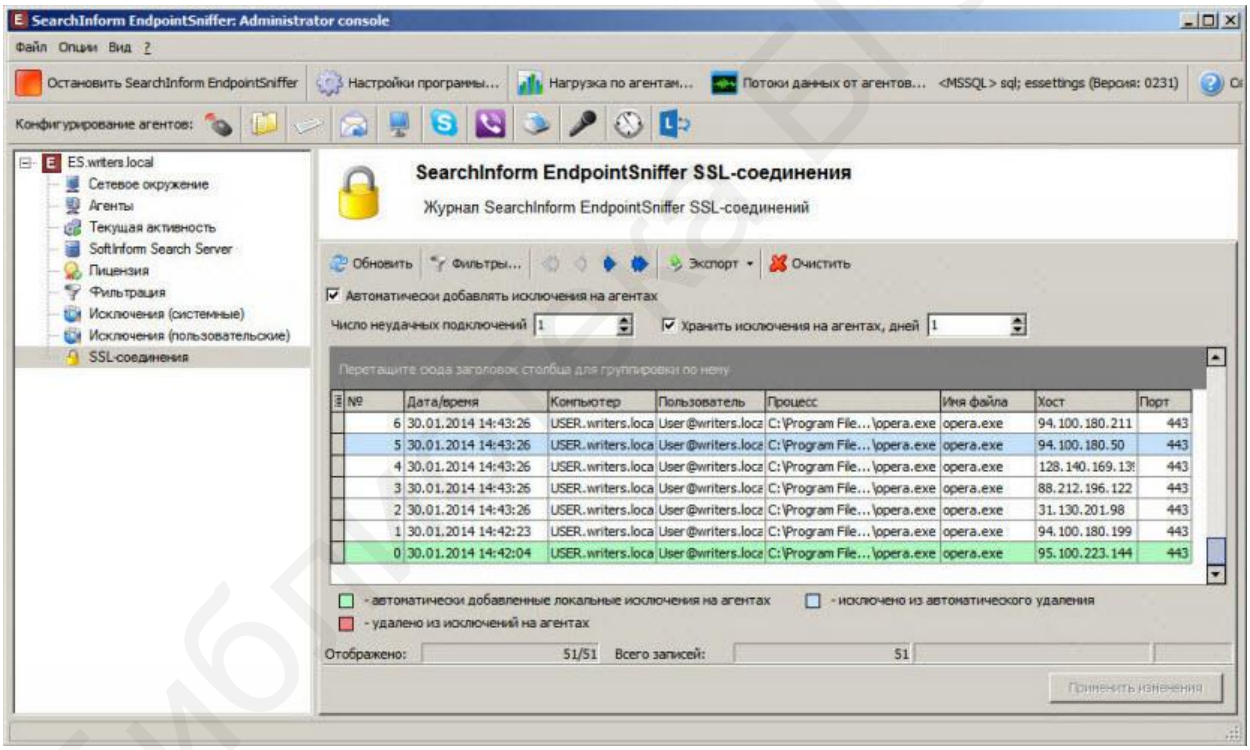


Рис. 2.125. Просмотр журнала соединений SSL

Для применения фильтрации к записям журнала SSL-соединений предназначена кнопка «Фильтры...». Записи журнала можно фильтровать по следующим параметрам (рис. 2.126):

– заданный временной интервал (дата и время);
– имя компьютера;
– доменный пользователь;
– процесс;
– хост;

– порт;

– тип (все, не автоматически добавленные, автоматически добавленные).

Для изменения любых настроек в окне «Фильтры» в нем должен быть установлен флажок в строке «Включить фильтр». Для указания в настройках фильтрации временного интервала должен быть установлен флажок в строке «Дата/время». Для фильтрации по другим параметрам необходимо задать соответствующее значение в полях «Компьютеры», «Пользователи», «Процессы», «Хосты», «Порты», «Тип». Для одного параметра можно задать несколько значений (через запятую). Чтобы расширить диапазон поиска, при вводе значения можно воспользоваться маской, например, *\IEXPLORE.EXE.

Для удаления всех настроек фильтрации следует нажать кнопку «Очистить». Результаты журнала SSL-соединений могут быть экспортированы в файл. Для этого необходимо нажать кнопку «Экспорт» и выбрать формат файла, в котором будут сохранены данные (HTML, TXT или XLS). В открывшемся окне сохранения файла следует указать, где будет располагаться файл с сохраненным журналом SSL-соединений. Для удаления выделенных записей журнала SSL-соединений служит кнопка «Очистить».

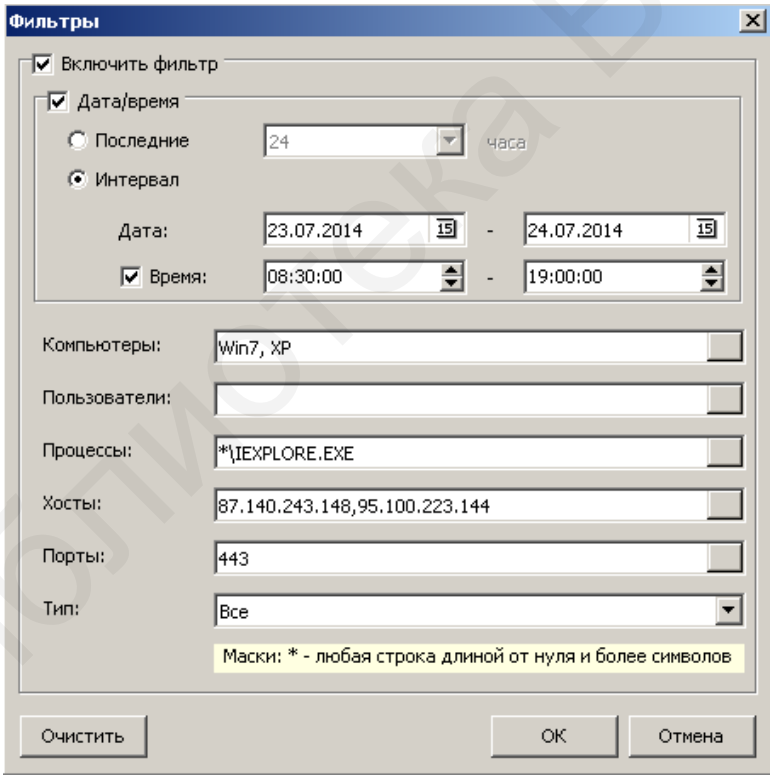


Рис. 2.126. Применение фильтрации к записям журнала SSL-соединений

Библиотека БГУИР

2.5. Управление индексами и базами данных компонентов программного комплекса «Контур информационной безопасности SearchInform» при помощи средств SearchInform DataCenter

Общая характеристика продукта SearchInform DataCenter [3]. Программный продукт SearchInform DataCenter входит в состав КИБ и предназначен для автоматизированного и ручного управления различными аспектами работы КИБ.

Перечень ключевых функций SearchInform DataCenter.

– управление индексами и базами данных продуктов;

– контроль работоспособности КИБ;

– управление службами компонентов КИБ;

– мониторинг дискового пространства на серверах КИБ;

– автоматическое оповещение о важных событиях;

– синхронизация с одним или более доменом Active Directory;

– разграничение прав доступа сотрудников службы безопасности к информации определенных пользователей или групп пользователей;

– задание настроек для подключения к базам данных по умолчанию;

– управление настройками компонентов КИБ.

Принцип работы SearchInform DataCenter. Принцип работы SearchInform DataCenter продемонстрирован на рис. 2.127.

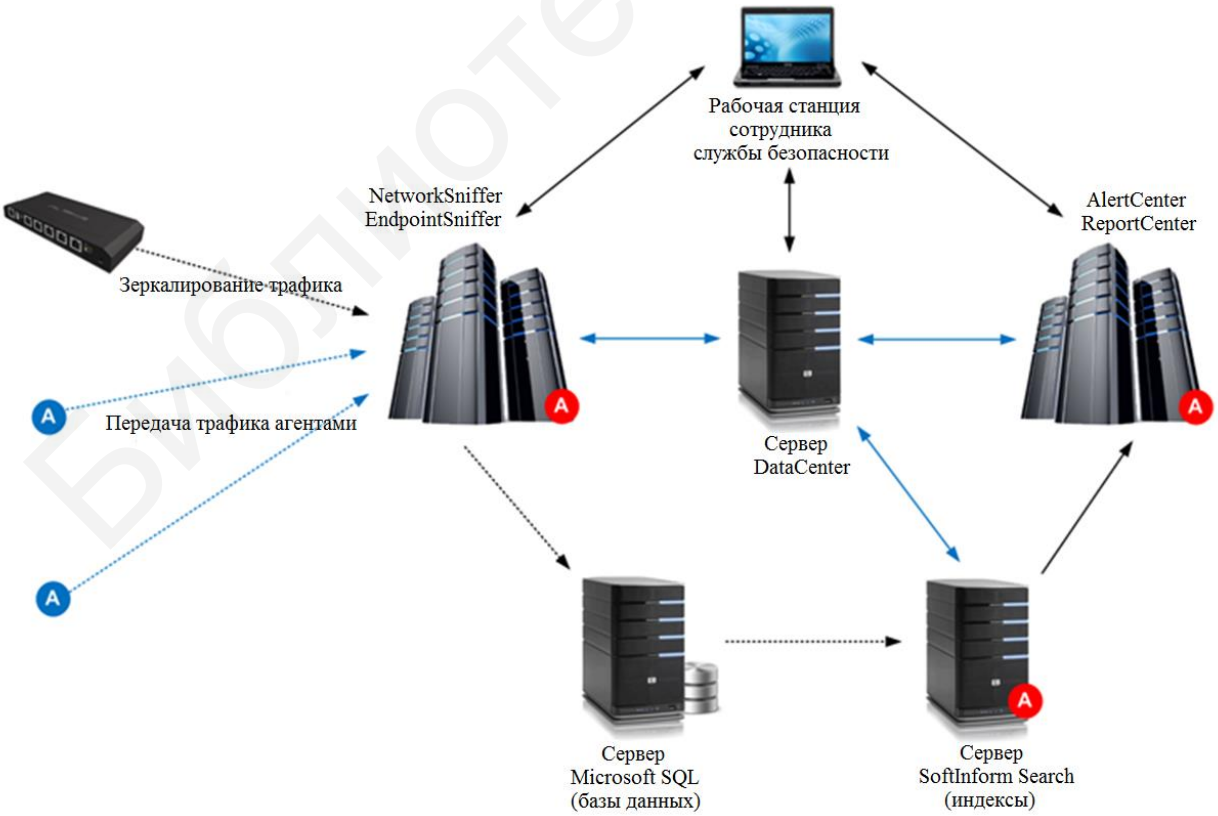


Рис. 2.127. Принцип работы SearchInform DataCenter

Библиотека БГУИР

На серверы компонентов DLP-системы «Контур информационной безопасности SearchInform» устанавливаются агенты DataCenter. Агенты периодически (с частотой 15–180 с в зависимости от состояния сети) проверяют статус контролируемых компонентов и передают сводку данных серверу DataCenter. Сервер DataCenter проверяет полученные данные в соответствии со своими настройками. Если требуется вмешательство, сервер передает команду агентам. Агент осуществляет требуемую операцию с контролируемым компонентом. Список поддерживаемых компонентов и продуктов КИБ представлен в табл. 2.11.

Таблица 2.11

Компоненты и продукты КИБ, поддерживаемые SearchInform DataCenter

Компонент	**Продукт**	**Функция**
1	**2**	**3**
SearchInform NetworkSniffer	HTTPSniffer	Перехват HTTP
	IMSniffer	Перехват мгновенных сообщений
	MailSniffer	Перехват электронной почты
	FTPSniffer	Перехват FTP
	CloudSniffer	Перехват файлов облачных сервисов
SearchInform NetworkSniffer Mail servers integration	MailSniffer	Интеграция с почтовыми серверами
SearchInform NetworkSniffer SMTP Mail servers integration	MailSniffer	SMTP-интеграция с почтовыми серверами
SearchInform ADSniffer	ADSniffer	Отслеживание и сохранение критичных событий из журналов безопасности Windows
SearchInform EndpointSniffer	HTTPSniffer	Перехват HTTP
	IMSniffer	Перехват мгновенных сообщений
	MailSniffer	Перехват электронной почты
	FTPSniffer	Перехват FTP
	SkypeSniffer	Перехват сообщений, файлов и голосовых сеансов связи программы Skype
	PrintSniffer	Перехват документов, отправленных на печать
	DeviceSniffer	Управление внешними устройствами и перехват данных, передаваемых на внешние устройства
	FileSniffer	Контроль операций с файлами, хранящимися на серверах и в общих сетевых папках
	MonitorSniffer	Перехват информации, отображаемой на мониторах пользователей

Библиотека БГУИР

Окончание табл. 2.11

1	2	3
	MicrophoneSniffer	Запись разговоров сотрудников как внутри, так и за пределами офиса
	KeyloggerSniffer	Отслеживание и сохранение логов нажатия клавиш и их комбинаций в любых приложениях
	LyncSniffer	Контроль текстового и голосового трафика, а также файлов, отправляемых посредством MS Lync
	ProgramSniffer	Мониторинг активности пользователей и процессов в течение рабочего дня
	ViberSniffer	Контроль текстового и голосового трафика, а также файлов, отправляемых посредством Viber
	CloudSniffer	Перехват файлов облачных сервисов
SearchInform DeviceSniffer	DeviceSniffer	Перехват данных, передаваемых на внешние устройства, с помощью сторонних продуктов DeviceLock / Lumension Device Control / Symantec DLP
SearchInform AlertCenter	AlertCenter	Автоматизированный анализ проиндексированных данных согласно заданным политикам безопасности
SearchInform ReportCenter	ReportCenter	Генерация отчетов по активности пользователей и по статистике инцидентов информационной безопасности
SoftInform Search Server	Search Server	Индексирование новых данных и поддержание индексов в актуальном состоянии

Консоль SearchInform DataCenter. Консоль позволяет осуществлять следующие операции:

– запуск и остановку сервера;

– настройку подключения к удаленному серверу;

– задание БД по умолчанию;

– настройку сервера;

– настройку параметров дискового пространства;

– синхронизацию КИБ с Active Directory операционной системы Windows;

– настройку прав доступа для сотрудников службы безопасности;

– автоматизацию операций с индексами и создание новых БД при выполнении заданных условий;

Библиотека БГУИР

– настройку оповещений по электронной почте по заданным критериям;

– автоматизацию управления продуктами.

Запуск и остановка сервера. Под запущенным сервером понимается работающая служба сервера DataCenter. Запуск и остановку сервера DataCenter можно произвести следующими способами:

– при помощи клиента DataCenter (графического интерфейса, предназначенного для управления сервером);

– при помощи оснастки «Службы».

Запуск сервера производится только на том компьютере, на который установлен сервер. Для запуска удаленного сервера можно использовать RDP-подключение.

Для запуска и остановки сервера при помощи клиента DataCenter необходимо нажать кнопку «Запустить», расположенную на вкладке «Управление» (рис. 2.128). При этом имя кнопки изменится на «Остановить».

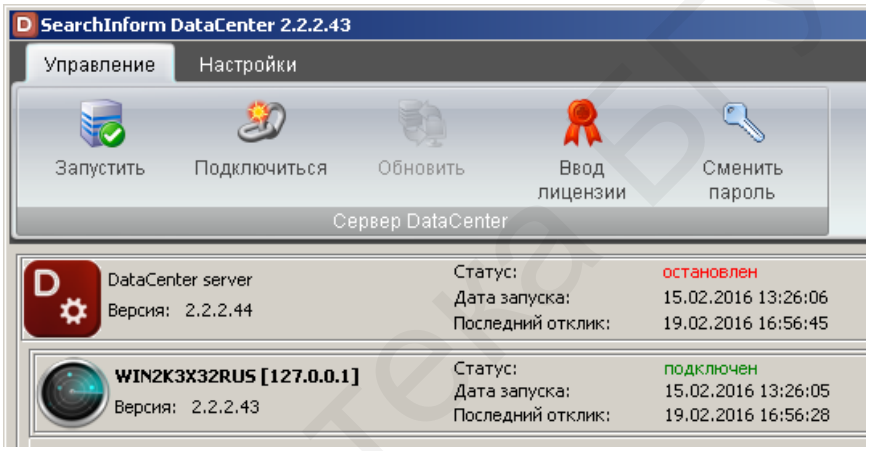


Рис. 2.128. Запуск сервера при помощи клиента DataCenter

Для запуска и остановки сервера при помощи оснастки «Службы» необходимо открыть оснастку «Службы», сочетанием клавиш Win+R вызвать окно «Выполнить» и выполнить команду services.msc. После этого следует запустить службу DCServer (рис. 2.129).

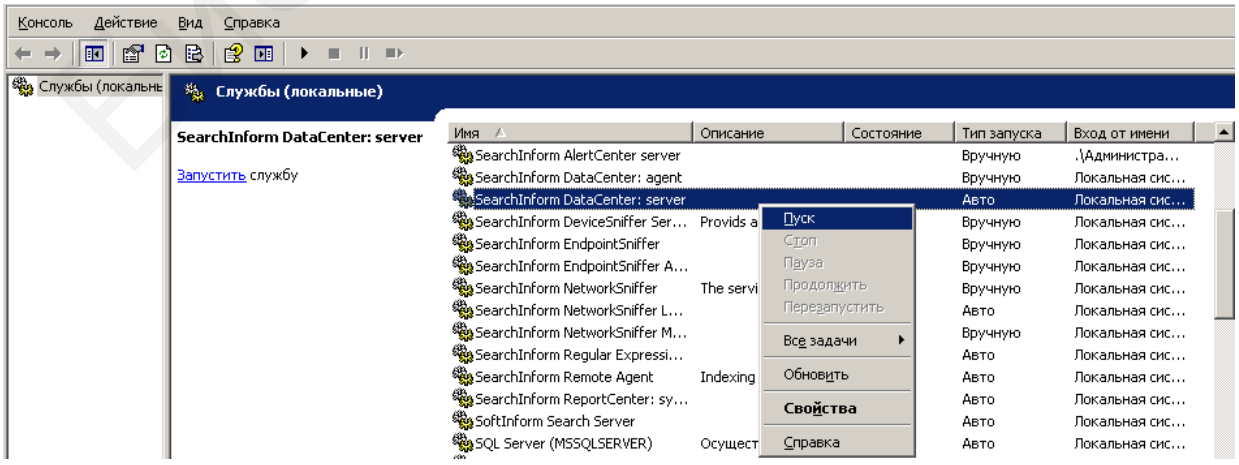


Рис. 2.129. Запуск сервера при помощи оснастки «Службы»

Если сервер запущен из оснастки «Службы», то при последующем вызове локального клиента потребуется произвести повторный запуск сервера.

В случае если клиент установлен удаленно от сервера (удаленный клиент должен иметь тот же пароль, что и клиент, установленный совместно с сервером), для подключения к удаленному серверу DataCenter необходимо выполнить действия в следующем порядке:

– нажать кнопку «Подключиться» (рис. 2.130);

– ввести IP-адрес или имя сервера DataCenter;

– клиент DataCenter может подключаться только к работающему серверу, поэтому, если отображается сообщение об ошибке, произвести запуск сервера.

При успешном подключении в консоли отобразится сервер DataCenter со списком управляемых приложений.

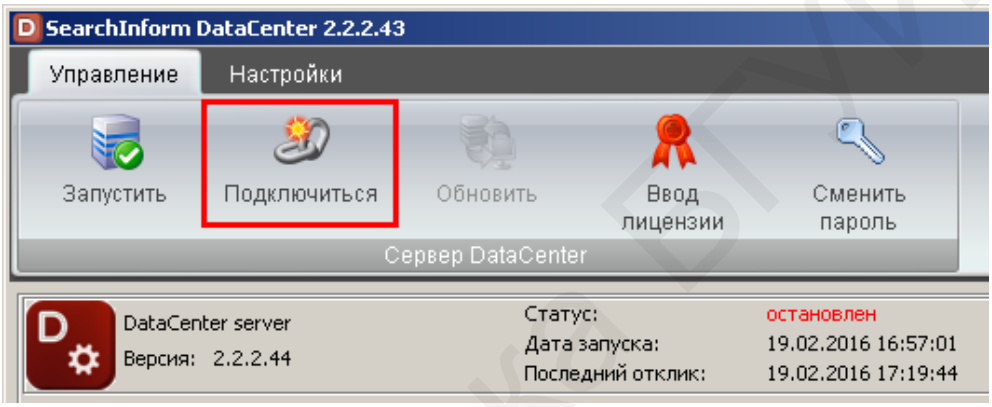


Рис. 2.130. Подключение к удаленному серверу DataCenter

Задание БД по умолчанию. DataCenter позволяет задать настройки для подключения к серверу баз данных под управлением СУБД MS SQL, которые считываются и подставляются в одноименные поля по нажатии кнопки «Считать из DataCenter». Для этого необходимо нажать кнопку «Базы данных по умолчанию» на вкладке «Настройки» и ввести параметры подключения к серверу MS SQL (рис. 2.131).

Проверить подключение к серверу можно, нажав кнопку «Проверка подключения».

Также DataCenter позволяет сгенерировать имя БД по следующим заданным параметрам:

– добавление указанного префикса перед наименованием БД;

– определение идентификатора сервера, на котором установлен компонент (актуально, когда система имеет несколько серверов данного компонента);

– выбор суффикса, добавляемого к имени БД (в зависимости от компонента).

Конечный вариант имени БД можно отредактировать вручную.

Настройки сервера. Для настройки параметров сервера следует перейти на вкладку «Настройки» и нажать кнопку «Сервер DataCenter» (рис. 2.132). Доступные настройки приведены в табл. 2.12.

Библиотека БГУИР

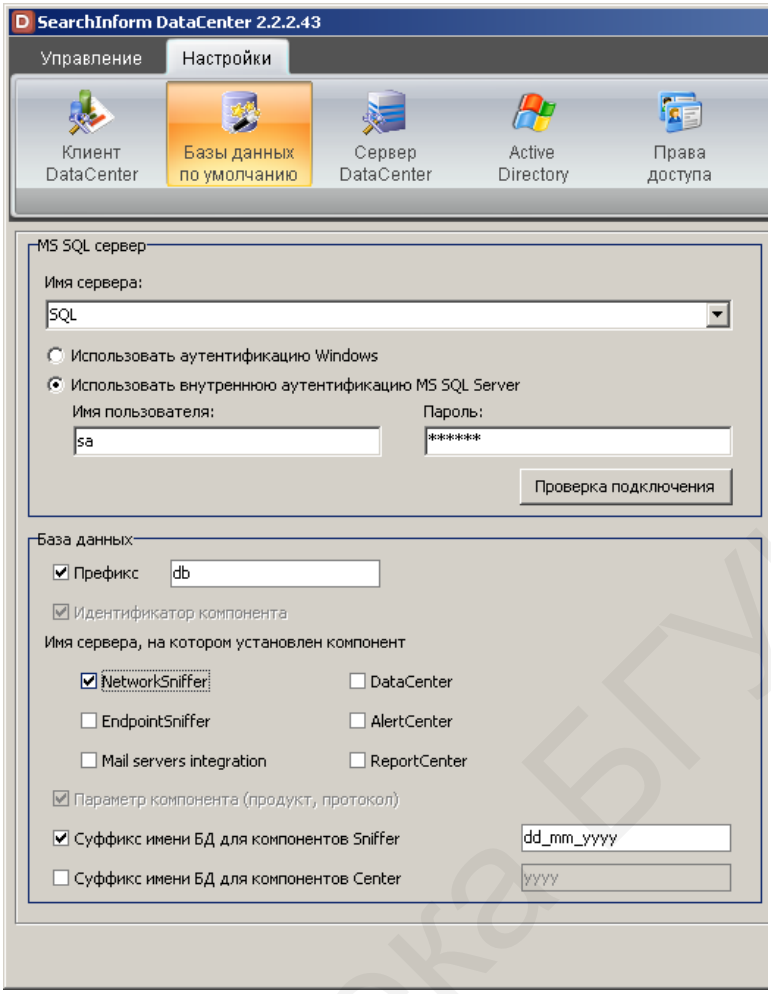


Рис. 2.131. Задание БД по умолчанию

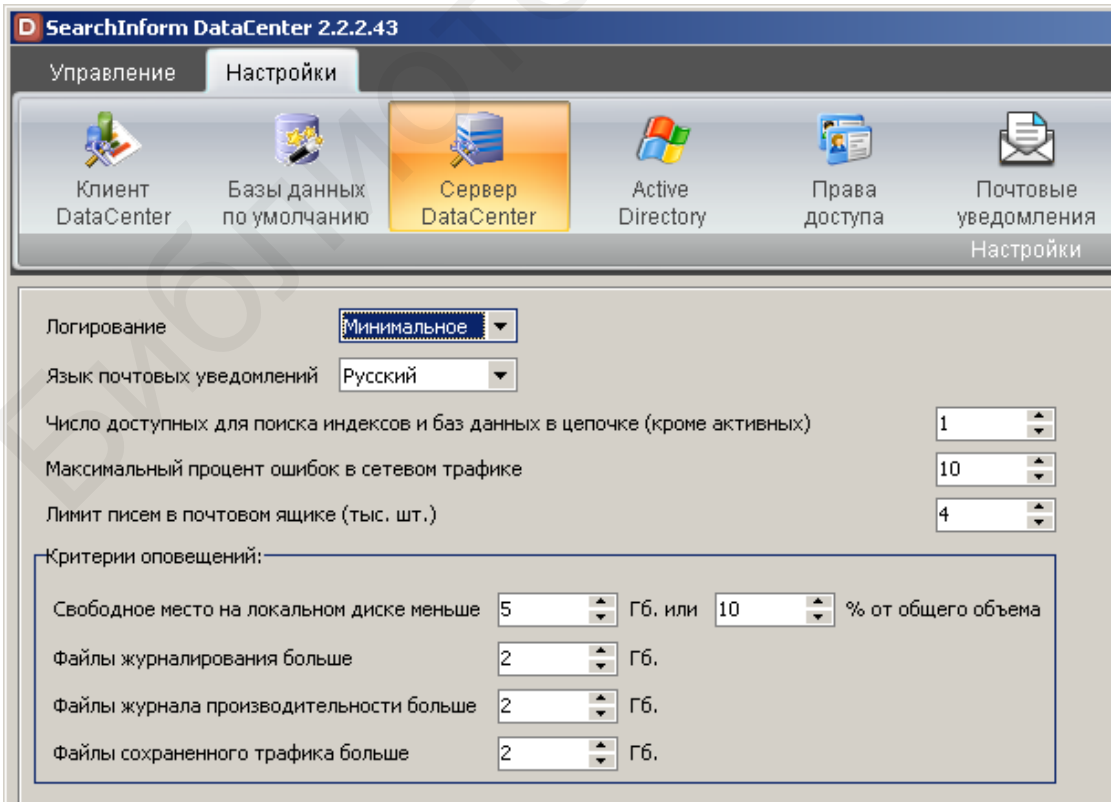


Рис. 2.132. Настройки сервера DataCenter

Библиотека БГУИР

Таблица 2.12

Настройки сервера DataCenter

Параметр	Значение	Функции
1	**2**	**3**
Логирование	Выключено	Протоколирование работы сервера DataCenter не производится
	Минимальное	Данный режим используется по умолчанию. Фиксируются только ошибки сервера DataCenter
	Обычное	Данный режим может быть включен при необходимости контроля работы сервера. Дополнительно к событиям, протоколируемым в нормальном режиме, фиксируются запуск и остановка служб и основных модулей программы
	Подробное	При включении данного режима фиксируются все действия с сервером, а также подробные стек-логи ошибок. Данный режим следует включать только по запросу сотрудников службы технической поддержки в случае критических проблем при работе с сервером. Включение данного режима понизит производительность работы сервера DataCenter и общую производительность системы
Число доступных для поиска индексов и БД в цепочке (кроме активных)		Ограничение по числу индексов, доступных для поиска. Активные индексы, в которые на данный момент сохраняются перехваченные документы, не учитываются
Язык почтовых уведомлений	Русский	Язык, на котором будут генерироваться сообщения сервера DataCenter
	English	
	Polski	
Максимальный процент ошибок в сетевом трафике		Ограничение процента возможных дублей пакетов в сетевом трафике, полученном сервером NetworkSniffer в результате зеркалирования. В свою очередь, дублирование пакетов означает, что требуется пересмотр настроек аппаратного обеспечения
Лимит писем в почтовом ящике (тыс. шт.)		Ограничение количества сообщений на почтовых серверах, работающих в режиме интеграции с сервером NetworkSniffer

Также на рассматриваемой вкладке можно осуществить настройку критериев оповещения о следующих событиях:

– свободное место на жестком диске ниже заданной величины (задается в гигабайтах или процентах общей емкости); данный критерий применяется по отношению ко всем доступным внутренним и внешним (USB HDD) накопителям;

Библиотека БГУИР

– объем файлов журналирования превышает заданную величину (задается в гигабайтах);

– объем файлов журнала производительности превышает заданную величину (задается в гигабайтах);

– объем файлов сохраненного трафика превышает заданную величину (задается в гигабайтах).

В случае превышения установленных квот по объему файлов или недостатку дискового пространства будет сгенерировано оповещение и отправлено по электронной почте аудитору безопасности (при настроенном уведомлении «Предупреждение»). Кроме того, на вкладке «Управление» пиктограмма индикации текущего состояния соответствующего компонента изменится с  на  (рис. 2.133).

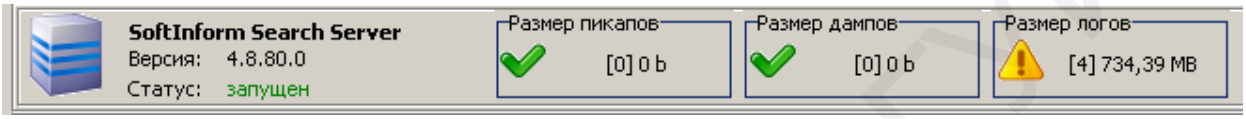


Рис. 2.133. Индикация превышения установленных квот по объему файлов или недостатку дискового пространства

Настройка синхронизации с Active Directory. Благодаря синхронизации с Active Directory компоненты КИБ могут считывать данные из БД DataCenter, поскольку обращение напрямую к Active Directory является долгим и достаточно неудобным процессом.

Существует возможность добавить как один, так и несколько доменов для синхронизации с Active Directory. Для добавления и удаления доменов предназначены кнопки  и  соответственно (рис. 2.134).

Настройки подключения к домену можно изменить, нажав кнопку  . Для ввода настроек подключения к БД необходимо воспользоваться кнопкой «Настройка подключения БД», после чего ввести данные для подключения к серверу (рис. 2.135). Также можно импортировать настройки подключения, воспользовавшись кнопкой «Считать из DataCenter». Кнопка «Проверка подключения» проверяет успешность подключения к БД.

Библиотека БГУИР

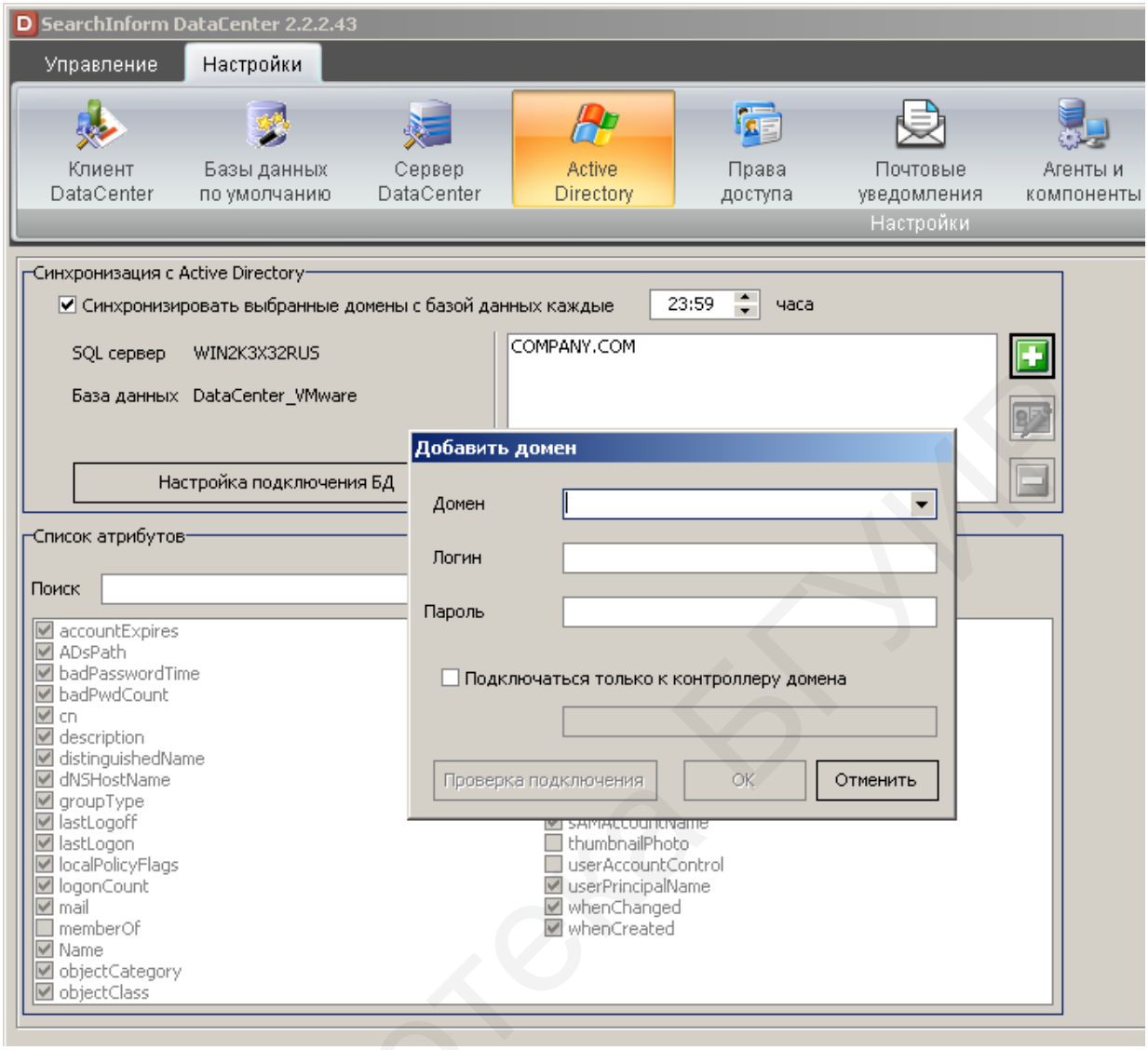


Рис. 2.134. Настройка синхронизации с Active Directory

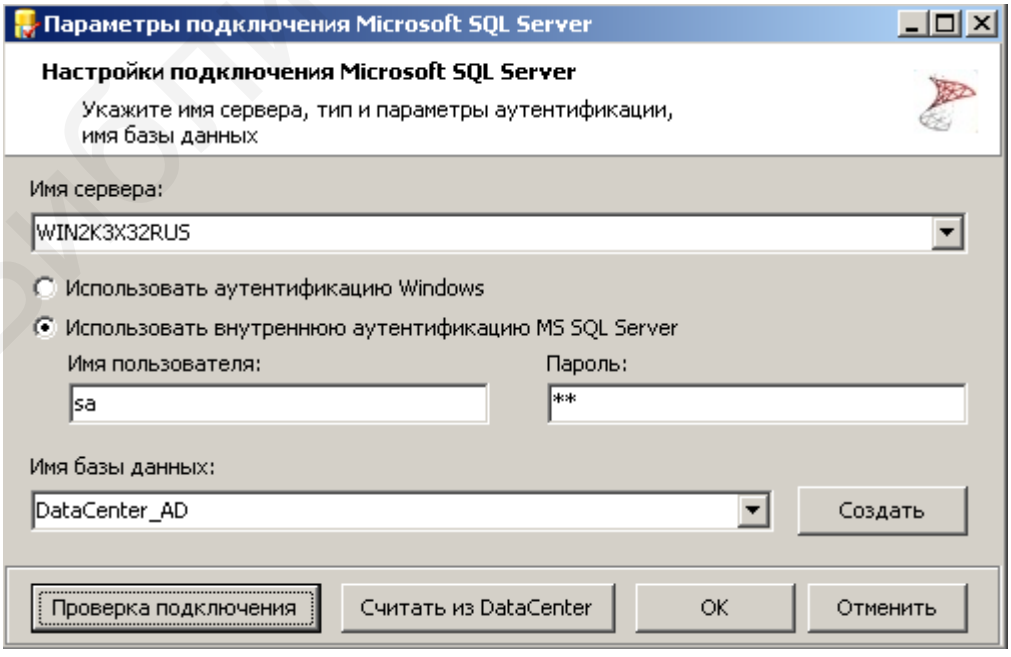


Рис. 2.135. Настройка подключения к БД

Библиотека БГУИР

Синхронизация с Active Directory запускается:

– при каждом запуске DataCenter;

– вручную на вкладке «Управление» по нажатии кнопки «Запустить»; при этом до окончания процесса синхронизации кнопка сменится на «Остановить» (рис. 2.136);

– каждые N часов согласно указанному времени в параметре «синхронизировать выбранные домены с базой данных каждые ... часа» (вкладки «Настройки», «Active Directory», группа настроек «Синхронизация с Active Directory (см. рис. 2.136)).

В нижней части вкладки «Active Directory» представлен список атрибутов Active Directory. Отмеченные флажками атрибуты DataCenter считывает и сохраняет в указанной БД.

Редактирование списка импортируемых в БД атрибутов в данной версии недоступно (доступны только поиск и сортировка по наименованиям).

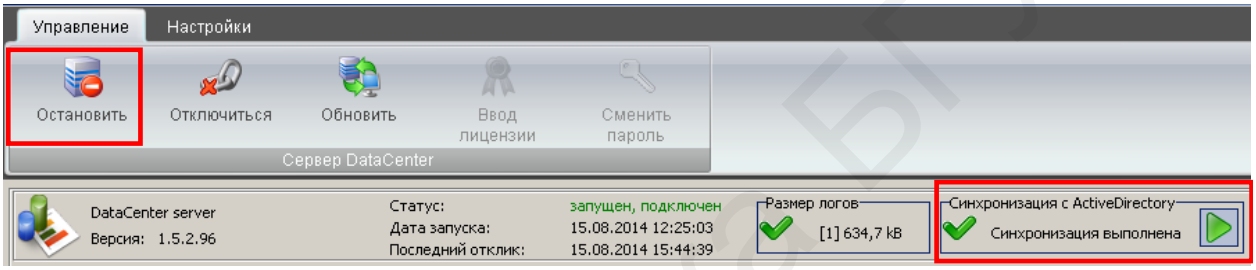


Рис. 2.136. Запуск синхронизации с Active Directory вручную

Разграничение прав доступа к данным. DataCenter позволяет создать список сотрудников службы безопасности и сформировать для каждого из них права на просмотр данных по тем или иным пользователям (или группам пользователей). Под данными подразумеваются инциденты, зафиксированные компонентом SearchInform AlertCenter, а также содержимое документов при просмотре в SearchInform Client.

Для управления правами доступа необходимо перейти на вкладку «Настройки» и нажать кнопку «Права доступа» (данная кнопка может быть неактивна, если в консоли DataCenter отключена синхронизация с Active Directory). В открывшемся информационном окне следует установить флажок в строке «Включить ограничение прав доступа для просмотра результатов поиска и инцидентов» (рис. 2.137). Правая часть окна разделена на две части: в верхней области можно составить список пользователей, которых может контролировать выбранный сотрудник службы безопасности, а в нижней области формируется список пользователей и компьютеров, права доступа к данным которых текущему аудитору безопасности иметь запрещено.

Библиотека БГУИР

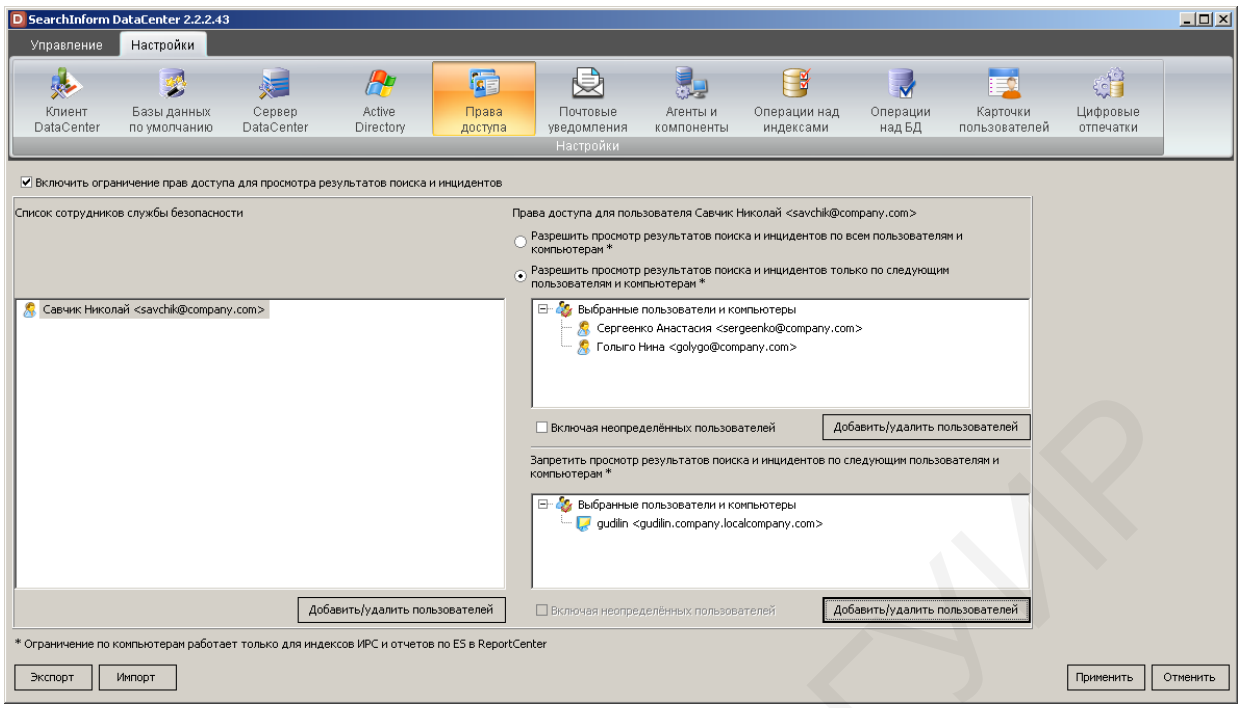


Рис. 2.137. Разграничение прав доступа к данным

Для выбора сотрудников службы безопасности из имеющегося списка в области «Список сотрудников службы безопасности» (левая часть информационного окна) необходимо нажать кнопку «Добавить/удалить пользователей», затем выделить в левой части добавленное имя сотрудника службы безопасности. После этого в правой части окна следует указать один из возможных режимов доступа:

– «Разрешить просмотр результатов поиска и инцидентов по всем пользователям»: при этом будет предоставлен неограниченный доступ (даже если пользователи в правой части не были выбраны);

– «Разрешить просмотр результатов поиска и инцидентов только по следующим пользователям»: в этом случае при помощи кнопки «Добавить/удалить пользователей» (в правой части окна) необходимо создать список пользователей, к данным которых сотрудник службы безопасности будет иметь доступ.

Флажок в строке «Включая неопределенных пользователей» предоставляет возможность просматривать документы пользователей, доменное имя которых системе не удалось определить, поэтому оно помечено как «unknown».

Для добавленных в список имен компьютеров ограничения будут применены только в отношении документов, проиндексированных на рабочих станциях пользователей, и отчетов по EndpointSniffer, доступных в клиентской консоли ReportCenter (отчеты по установленному ПО, истории установки ПО, истории установки агентов на рабочие станции).

Сохранить сделанные настройки можно, нажав кнопку «Применить». Отключение синхронизации с Active Directory, после того как были разграничены права доступа, влечет за собой деактивирование произведенных изменений.

Библиотека БГУИР

Настройка почтовых уведомлений. Сервер DataCenter позволяет оповещать пользователя о событиях DataCenter и управляемых компонентов по электронной почте. Для настройки параметров данной функции предназначена кнопка «Почтовые уведомления» на вкладке «Настройки» (рис. 2.138).

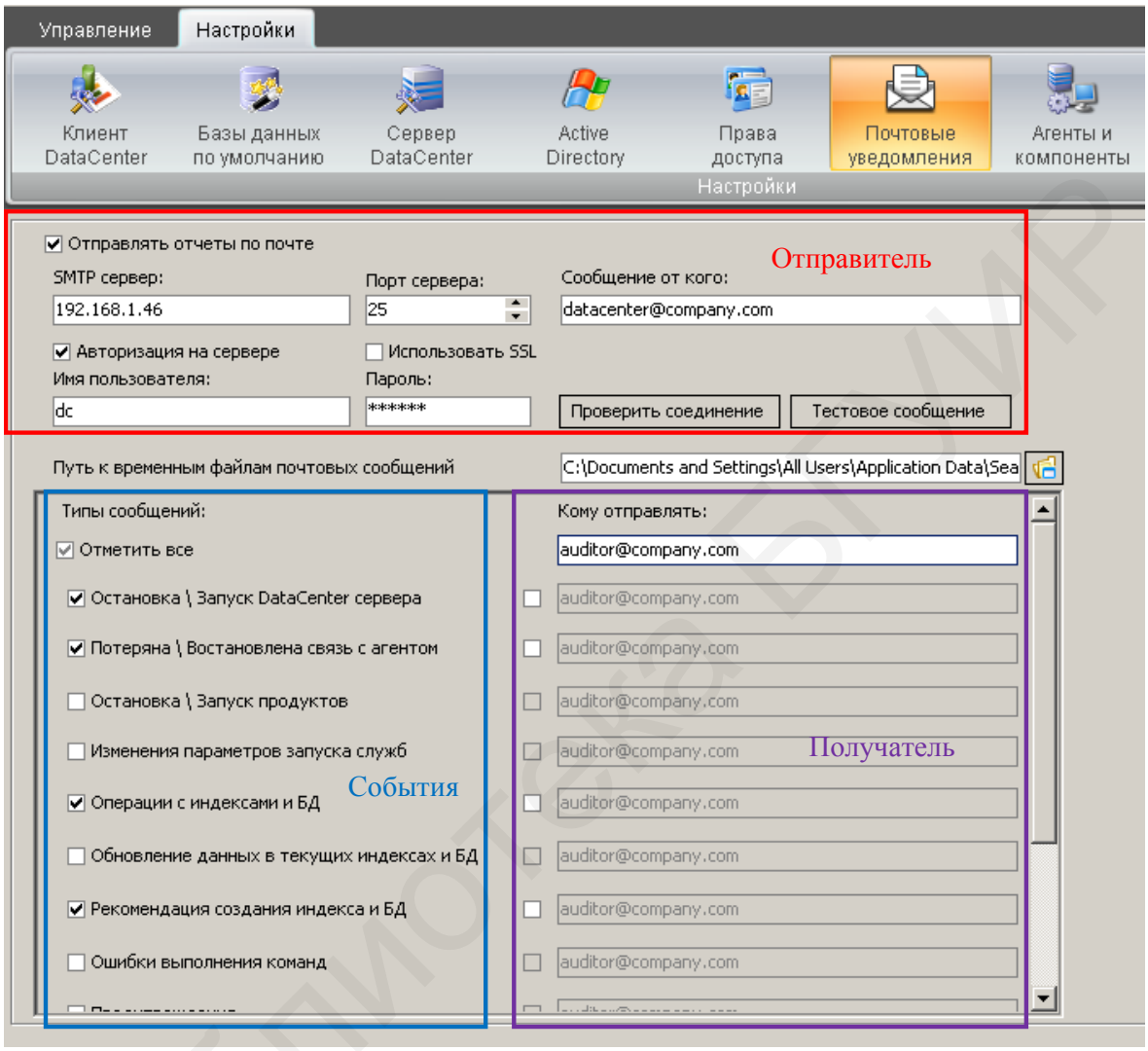


Рис. 2.138. Настройка почтовых уведомлений

Настройка почтовых уведомлений включает следующие действия:
– настройку отправителя почтовых сообщений;
– выбор событий;
– настройку получателей почтовых сообщений.
Настройка отправителя почтовых сообщений предполагает ввод:
– IP-адреса либо имени SMTP-сервера;
– значения порта ввода-вывода, используемого SMTP-сервером;
– адреса отправителя.

Если требуется аутентификация SMTP, необходимо установить флажок в строке «Авторизация на сервере» и ввести имя и пароль почтовой учетной записи. Кнопками «Проверить соединение» и «Тестовое сообщение» можно проверить корректность заданных настроек и наличие соединения с сервером.

Библиотека БГУИР

Список событий, для которых можно настроить уведомления, включает:

– остановку/запуск сервера DataCenter;

– потерю/восстановление связи с агентом;

– остановку/запуск продуктов;

– изменения параметров запуска служб;

– операции с индексами;

– обновление данных в текущих индексах;

– рекомендации создания нового индекса;

– ошибки выполнения команд;

– предупреждения (также используются для оповещений по дисковому пространству);

– создание файла журнала диагностики;

– уведомления NetworkSniffer;

– уведомления EndpointSniffer;

– уведомления ReportCenter.

Для выбора событий необходимо установить соответствующие флажки. Настройка получателей почтовых сообщений подразумевает ввод почтового адреса получателя по умолчанию в верхнее поле.

Если некоторые уведомления требуется отправлять по другому электронному адресу, следует установить соответствующие флажки и ввести новые адреса. Ввод нескольких адресов получателей уведомлений производится через запятую.

Автоматическое управление компонентами КИБ. При помощи DataCenter можно отслеживать состояние служб контролируемых компонентов и принудительно запускать их вне зависимости от того, по какой причине они были остановлены.

Для настройки автоматического включения служб компонентов необходимо осуществить следующие операции:

1) нажать кнопку «Агенты и компоненты» на вкладке «Настройки» (рис. 2.139);

2) раскрыть список установленных компонентов КИБ и установить флажок в строке «Автоматическое управление» для тех компонентов, службы которых должны включаться автоматически;

3) отметить флажком параметр «Запускать принудительно» напротив продукта, службы которого требуется запускать автоматически;

4) нажать кнопку «Применить».

Библиотека БГУИР

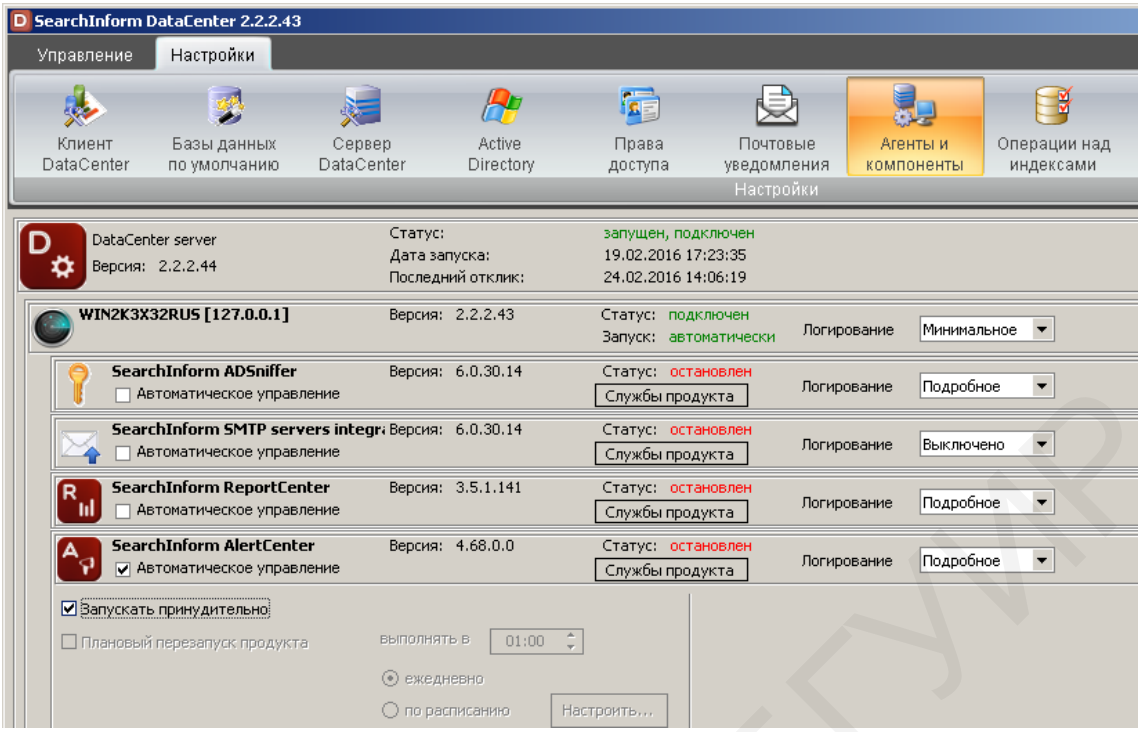


Рис. 2.139. Автоматическое управление компонентами

Если же параметр «Запускать принудительно» не отмечен флажком, то на вкладке «Управление» будет активна кнопка «Запустить/Остановить» (в зависимости от статуса компонента) для запуска/остановки его вручную (рис. 2.140).

Также существует возможность задания настроек планового перезапуска выбранного компонента. Для этого следует:

1) отметить флажком параметр «Плановый перезапуск продукта» напротив компонента, который требуется перезапускать автоматически;

2) настроить условия перезапуска:

– для ежедневного перезапуска компонента в назначенное время необходимо использовать параметр «Ежедневно», установив время перезапуска;

– для задания особого расписания перезапуска продукта – параметр «По расписанию» и кнопку «Настроить». В окне «Планировщик» указывается, по каким числам месяца или в какой день недели месяца будет производиться перезапуск продукта, а также устанавливается начальная дата операции (рис. 2.141).

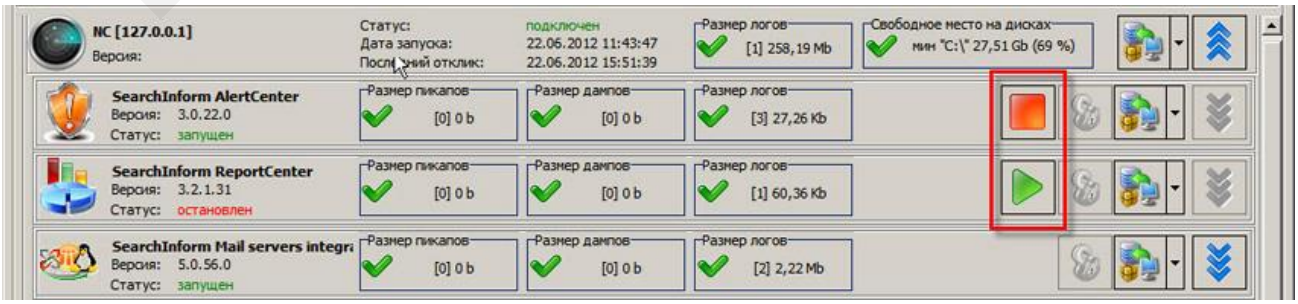


Рис. 2.140. Принудительный запуск/остановка компонентов

Библиотека БГУИР

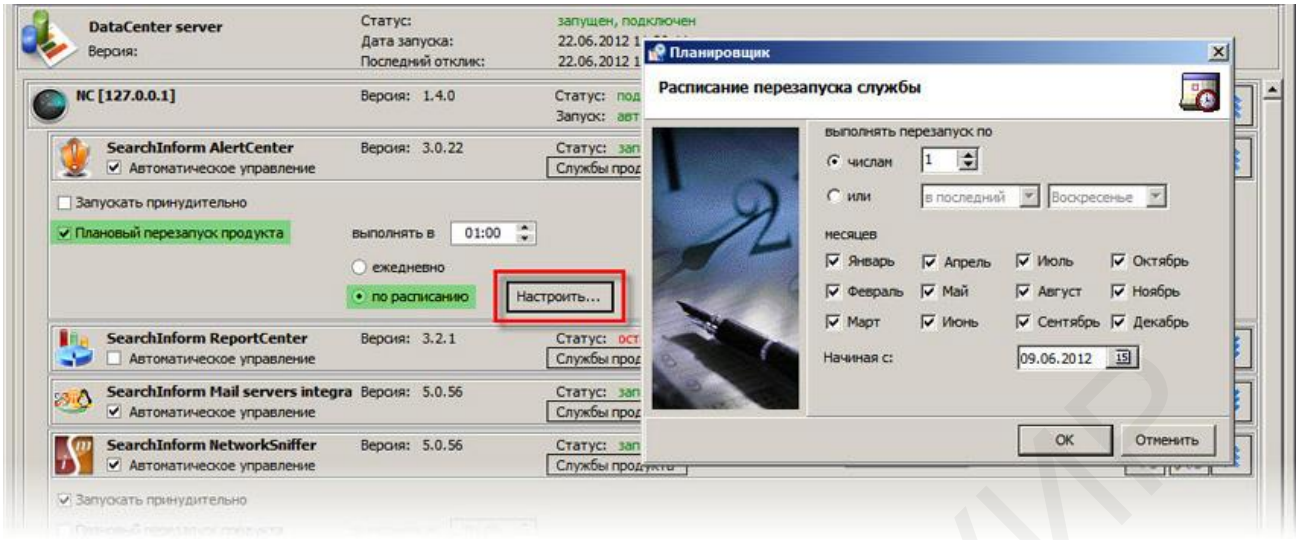


Рис. 2.141. Запуск компонентов по расписанию

Автоматическое управление индексами предполагает прежде всего ограничение их размера. Необходимость этого вызвана следующими причинами:

– по мере роста индекса поиск по нему замедляется;

– использование нескольких индексов среднего размера вместо одного индекса большого размера позволяет оптимизировать аналитическую обработку перехваченной информации;

– операции с большим индексом (обновление, дефрагментация) занимают больше времени, чем операции с малыми индексами;

– при значительном увеличении размера индекса увеличивается вероятность ошибок и утраты проиндексированных данных.

Все автоматические операции с индексами будут осуществляться лишь при условии активизации параметра «Автоматическое управление» у соответствующего компонента.

Для настройки автоматического управления индексами на вкладке «Настройки» следует нажать кнопку «Операции над индексами». Будет отображен список доступных для управления продуктов (рис. 2.142).

Далее следует выбрать продукт, для которого необходимо настроить правила, после чего установить флажок в строке «Автоматически создавать индексы по достижении условий».

Если создание новых индексов должно происходить только в заданные часы (например, в нерабочее время), следует установить флажок в строке «только в промежутке времени между» и настроить время. Также необходимо установить флажки для перечисленных далее критериев, по которым можно производить операции создания новых индексов, после чего ввести требуемые значения:

– максимальный размер индекса (Гб);

– максимальный размер перехваченных документов в индексе (Гб);

– максимальный размер перехваченных документов в базе данных (Гб);

Библиотека БГУИР

– максимальный размер текста перехваченных документов (Гб);
– максимальное число перехваченных документов (млн);
– максимальное число записей в базе данных (млн);
– максимальное число уникальных слов (млн)
– максимальный возраст индекса (дней);
– по расписанию.

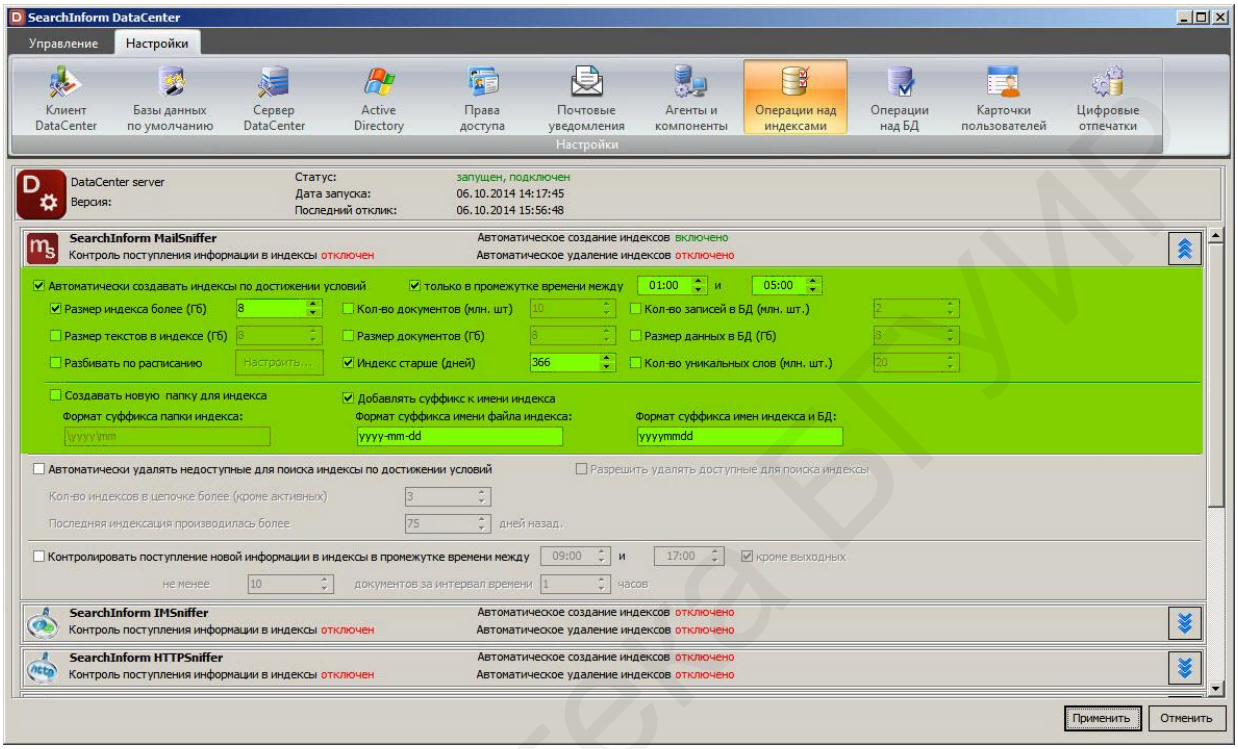


Рис. 2.142. Автоматическое управление индексами

Для настройки автоматического разбиения индексов по расписанию (рис. 2.143) используются флажок в строке «Разбивать по расписанию» и кнопка «Настроить». Доступны следующие настройки:

– число месяца или день недели (первый/второй/третий/четвертый/последний) + (понедельник – воскресенье) определенного месяца;

– дату, с которой расписание будет включено;

– минимальный возраст индекса в днях (операция будет отменена, если возраст индекса меньше указанного значения).

При создании папок для индексов и настройке суффиксов имен индексов и БД следует пользоваться приведенными далее рекомендациями.

1. При создании индексов существует возможность настройки их сохранения как в текущую, так и в новую папку. В суффиксах папок, индексов и баз данных можно использовать переменные («yyyy» – год, «mm» – месяц, «dd» – день месяца, «hh» – час, «nn» – минуты, «ss» – секунды). В качестве разделителя используется знак «~».

2. По умолчанию функция помещения нового индекса в отдельную подпапку отключена. В случае же ее применения доступен формат суффикса

папки индекса по умолчанию – «\yyyy\mm» (например, \2014\08). Путь задается относительно папки с оригинальным индексом. Недопустимые символы – «/», «"», «|», «:», «*», «?», «<», «>».

3. Имя индекса не обязательно должно совпадать с именем файла индекса и именем БД. Суффикс можно привязать к дате и времени операции. Настройка по умолчанию – «mmddhhnnss». Настройка суффиксов производится при установленном флажке в строке «Добавлять суффикс».

4. Суффикс имени файла индекса вводится в поле «Формат суффикса имени файла индекса». Недопустимые символы – «/», «"», «|», «:», «*», «?», «<», «>», «\», «#», «~».

5. Суффикс имен индекса и БД вводится в поле «Формат суффикса имен индекса и БД».

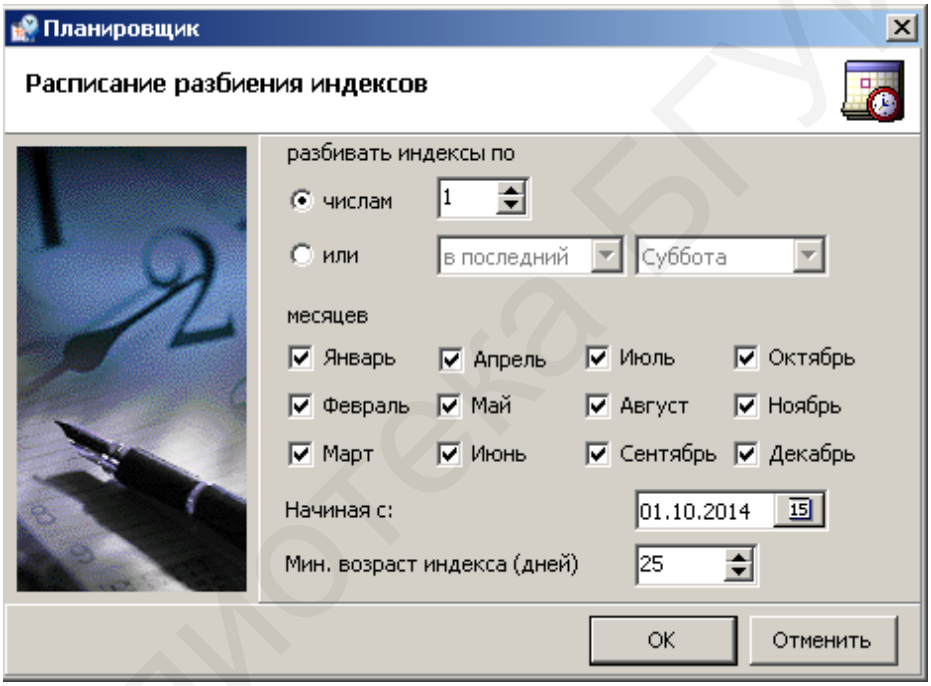


Рис. 2.143. Настройка автоматического разбиения индексов по расписанию

Для изменения пути к индексу следует установить флажок в строке «Создавать новую папку для индекса» и ввести путь к индексу в новом формате.

Для изменения суффикса имени файла индекса, имен базы данных и индекса необходимо установить флажок в строке «Добавлять суффикс к имени индекса» и ввести суффиксы в новом формате.

Переопределение настроек автоматического управления. Поскольку один и тот же продукт (например, MailSniffer) включен в несколько компонентов (EndpointSniffer, NetworkSniffer, Mail servers integration, SMTP servers integration), в консоли каждого из них создаются отдельные индексы. Данные, хранящиеся в индексе, могут отличаться: одни из них получены в результате зеркалирования трафика, другие – получены с корпоративного почтового сервера, третьи – перехвачены агентом. Однако при активизирован-

Библиотека БГУИР

ном параметре автоматического управления продуктами операции (создание, удаление, контроль поступления данных) будут производиться для всех индексов продукта без исключения. Существует возможность задания отдельных настроек управления индексами для некоторых продуктов:

– EndpointSniffer – MailSniffer, FTPSniffer, IMSniffer, HTTPSniffer;
– NetworkSniffer – MailSniffer, FTPSniffer, IMSniffer, HTTPSniffer;
– Mail servers integration – MailSniffer;
– SMTP servers integration – MailSniffer.

Переопределение глобальных настроек производится на вкладке «Агенты и компоненты». Для этого необходимо установить флажок в строке «Автоматическое управление» напротив выбранного компонента и раскрыть список параметров. В правой части информационного окна следует отметить флажком продукт, к индексам которого будут переопределены настройки, после чего – нажать кнопку «Настроить» (рис. 2.144). Параметры, доступные в отобразившемся диалоговом окне, идентичны описанным ранее (см. рис. 2.142).

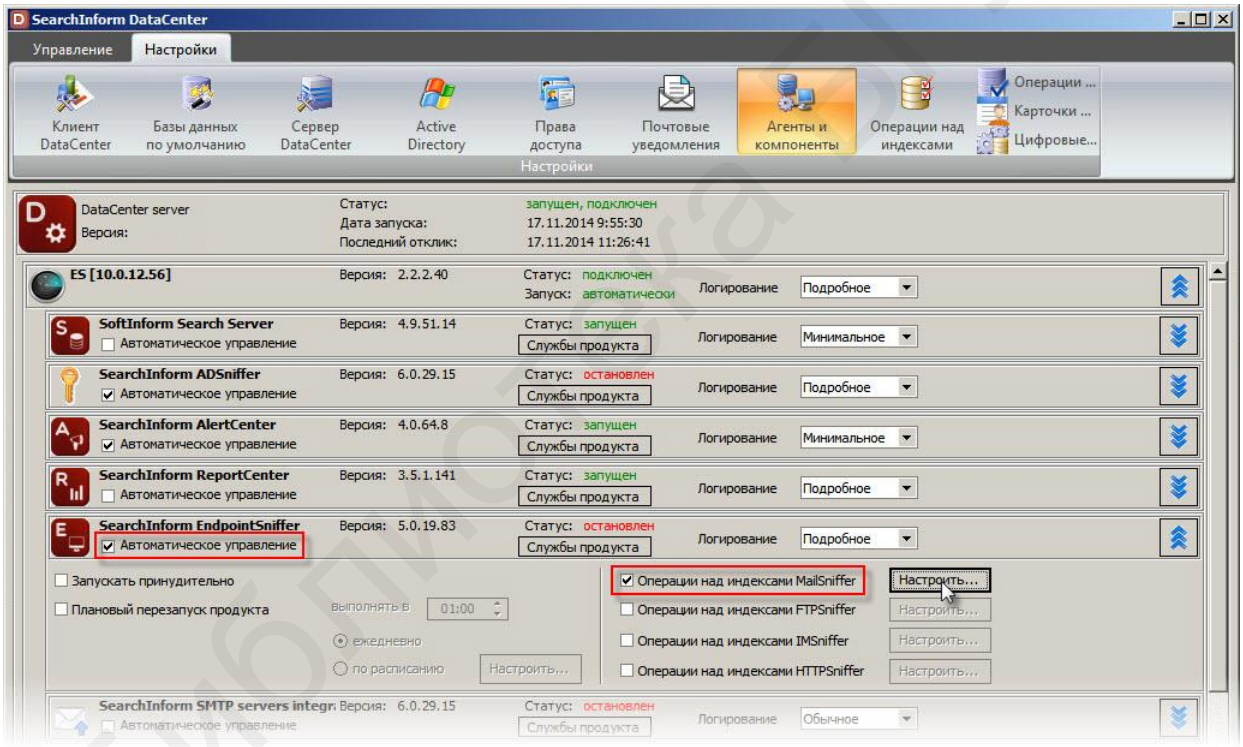


Рис. 2.144. Переопределение настроек автоматического управления

В рамках примера, приведенного на рис. 2.144, сделанные настройки будут применены только к почтовым индексам компонента EndpointSniffer, установленного на сервере ES. Для остальных индексов электронной почты будут по-прежнему действовать глобальные настройки вкладки «Операции над индексами» (если они заданы).

Также существует возможность настроить условия, при наступлении которых недоступные для поиска индексы будут автоматически удалены. Чтобы активировать указанную операцию, необходимо установить флажок напротив

параметра «Автоматически удалять недоступные для поиска индексы по достижении условий» (см. рис. 2.144). В качестве условий можно задавать:

– число индексов в цепочке, при превышении которого самый старый индекс может быть удален (минимальное значение – 2 шт.);

– количество дней с момента последней индексации баз данных (минимальное значение – 15 дней).

Индекс будет удален только по достижении обоих условий одновременно.

Дополнительно можно настроить возможность оповещения в случае отсутствия перехвата. Для этого необходимо установить флажок в строке «Контролировать поступление новой информации в индексы в промежутке времени между» (см. рис. 2.142) и ввести время, в течение которого производится контроль, например, 9:00 и 17:00 (для установки непрерывного контроля поступления перехваченных данных можно использовать промежуток времени 00:00–23:59). Далее следует указать минимальное требуемое число сообщений и интервал времени, за который эта информация должна поступить. Например, не менее 10 документов за 1 час (настройка по умолчанию). При этом минимальное значение времени составляет 1 час, максимальное – 72 часа.

Служба сбора данных осуществляет извлечение из атрибутов документов выбранных индексов (почтовых, IM, Skype, Lync, Viber) контактных данных и привязку их к внутреннему или внешнему пользователю компании. Данные по внутренним пользователям извлекаются из базы данных DataCenter, которые в свою очередь были импортированы из Active Directory. В дальнейшем полученная информация используется для генерирования и отображения карточек пользователей в приложении SearchInform Client.

Перейдите на вкладку «Настройки» → «Карточки пользователей» (рис. 2.145). В блоке настроек «Расписание» укажите частоту загрузки пользователей из Active Directory и импорта данных из индексов (при необходимости можно указать начальную дату для импортируемых индексов). Выберите уровень логирования службы сбора данных.

Отметьте флажками индексы, из которых будет извлекаться информация. Если необходимо собирать данные всех индексов без исключения, установите флажок напротив параметра «Обрабатывать все доступные индексы (mail, skype, im, lync, viber)».

Управление службой сбора данных производится с помощью следующих кнопок:

– «Остановить» – остановка работающей службы;

– «Запустить» – старт службы;

– «Перезапустить» – перезапуск службы.

Управление базой данных производится с помощью следующих команд:

– «Очистить базу данных» – удаление извлеченной информации из базы данных DataCenter;

– «Загрузить индексы заново» – извлечение всех данных из индекса заново.

Библиотека ГГТУ им

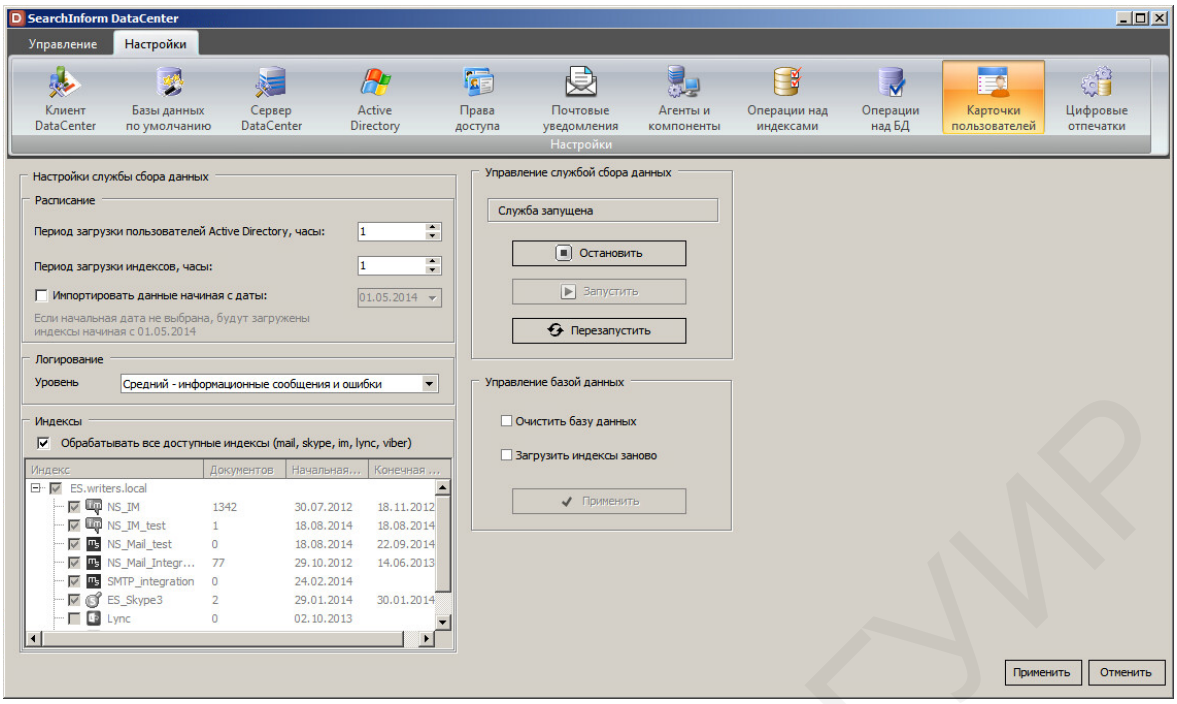


Рис. 2.145. Карточки пользователей

Цифровые отпечатки позволяют отслеживать утечку конфиденциальной информации на основании сформированного набора эталонных документов (образцов), содержащих текстовую информацию, например, устава компании, реестра держателей акций, финансовых отчетов и т. п. Перехваченные данные сопоставляются с содержанием документов-образцов.

При описании технологии работы с цифровыми отпечатками используется следующая терминология:

1. Каталог образцов – категории, используемые для группировки образцов по тематике или другим признакам. Можно использовать один каталог или несколько каталогов.

2. Образцы – документы, используемые в качестве контрольных при проверке перехваченной информации. Это могут быть файлы любых форматов, в том числе и основных графических, содержащих текстовую информацию. Однако для более точного поиска рекомендуется использовать текстовые форматы (DOC, TXT), не содержащие таблиц. Минимальный размер образца – одно-два развернутых предложения со знаками препинания. Чем объемнее образец, тем более точными будут результаты поиска.

3. Папки образцов – локальные или сетевые папки, в которых хранятся образцы.

4. Индекс FingerPrints – специальный индекс, используемый для сравнения перехваченных документов с образцами. Индекс является служебным, в отличие от основного, который формируется сервером индексации и может подключаться к базам AlertCenter.

5. Индексация – процедура создания или обновления индекса цифровых отпечатков.

6. Расписание обновления – расписание, по которому индекс отпечатков синхронизируется с образцами.

Библиотека БГУИР

Для работы с цифровыми отпечатками необходимо создать каталог образцов документов (либо использовать уже имеющийся). Перейдите на вкладку «Цифровые отпечатки» и в группе настроек «Каталог образцов цифровых отпечатков» нажмите кнопку «Добавить» (рис. 2.146).

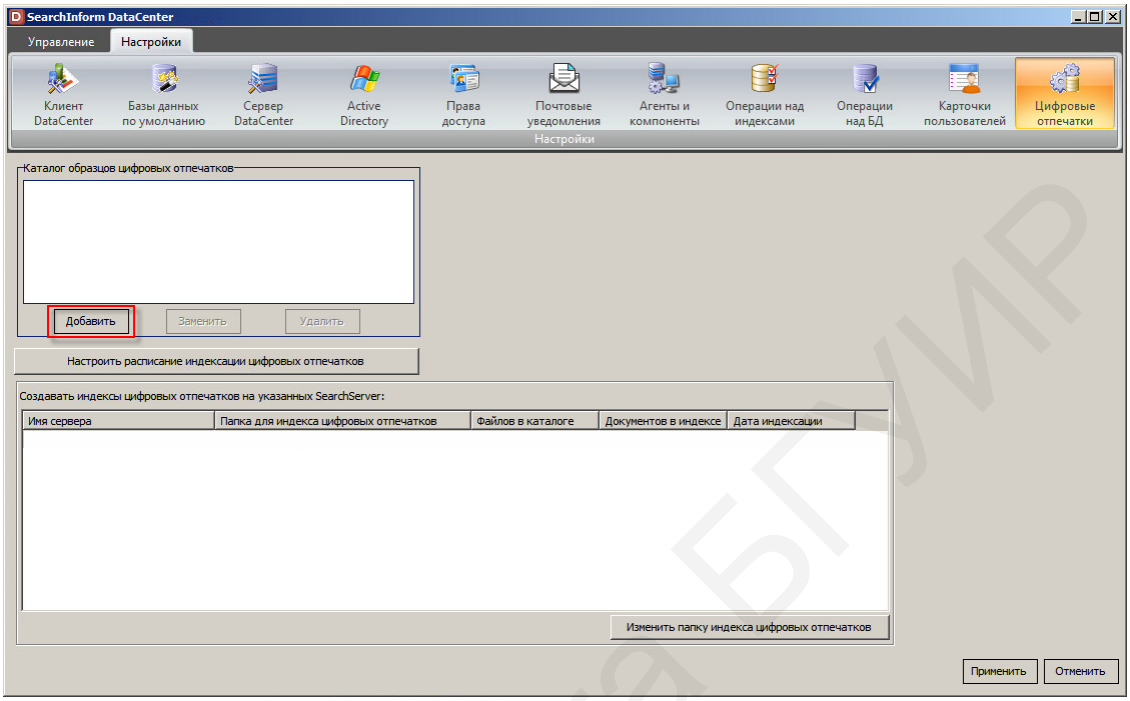


Рис. 2.146. Вкладка «Цифровые отпечатки»

Выберите папку в появившемся окне и нажмите «ОК» (рис. 2.147).

Каталог образцов цифровых отпечатков будет отображен в списке. Для изменения выбранной папки предназначена кнопка «Заменить», для удаления – «Удалить». Нажмите кнопку «Настроить расписание индексации цифровых отпечатков» (см. рис. 2.146).

Для выбора периодичности проверки предназначены опции «Ежедневно», «Еженедельно», «Ежемесячно», «Единовременно» и «По настройке». Если установлен флажок в строке «Расписание включено», индексация будет запущена немедленно по завершении работы мастера (рис. 2.148).

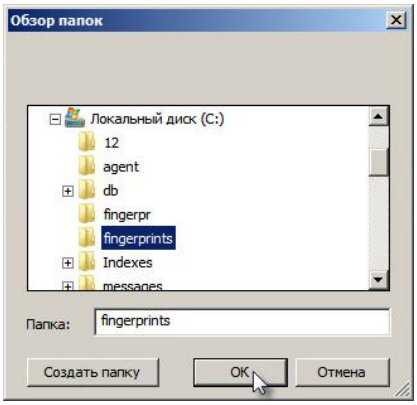


Рис. 2.147. Выбор папки

Библиотека БГУИР

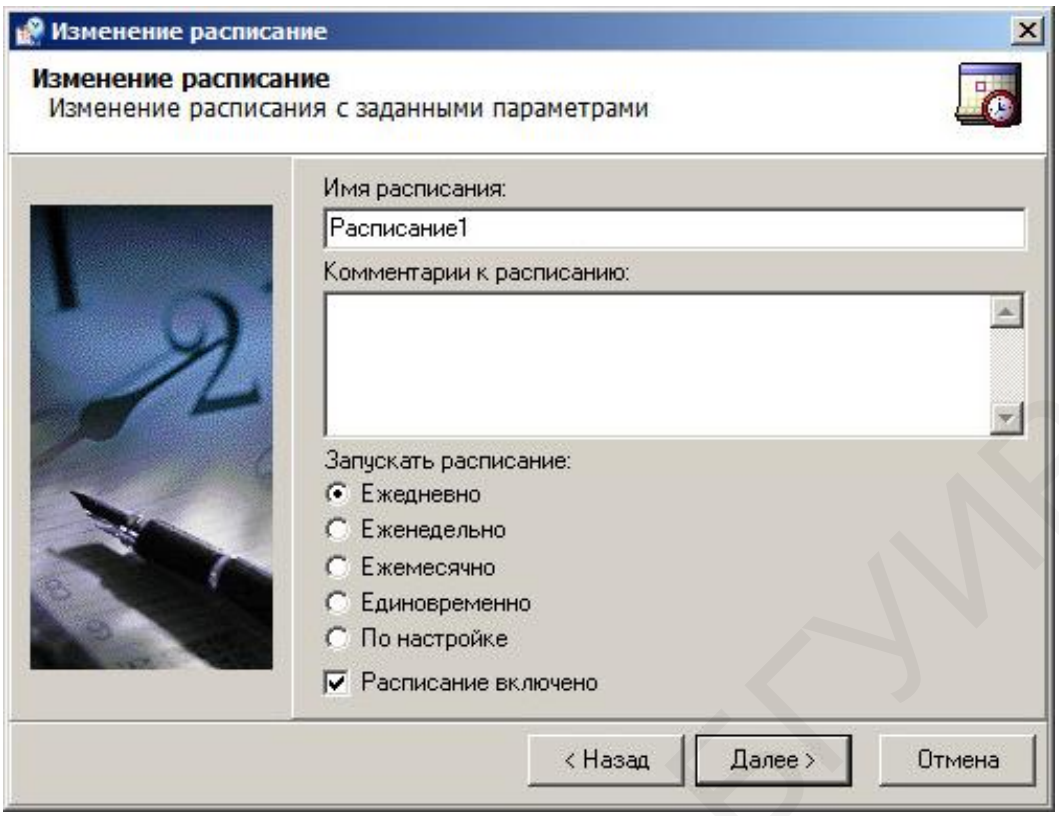


Рис. 2.148. Задание расписания

Далее настройте расписание обновления.

Установите флажок напротив в строке SoftInform Search, на котором требуется создать индекс FingerPrint. Директория для сохранения индекса может быть изменена после нажатия кнопки «Изменить папку индекса цифровых отпечатков» (рис. 2.149).

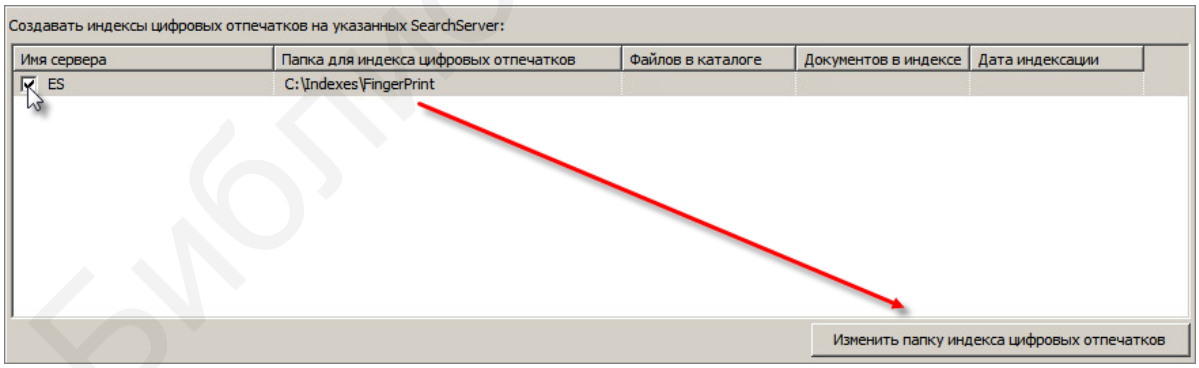


Рис. 2.149. Изменение папки цифровых отпечатков

Нажмите кнопку «Применить» в нижней части консоли (рис. 2.150).

По истечении некоторого времени будет отображено количество файлов в каталоге образцов, а в заданной папке появится индекс FingerPrint_NPM. Одноименный индекс будет отображен в консоли сервера SoftInform Search.

Библиотека БГУИР

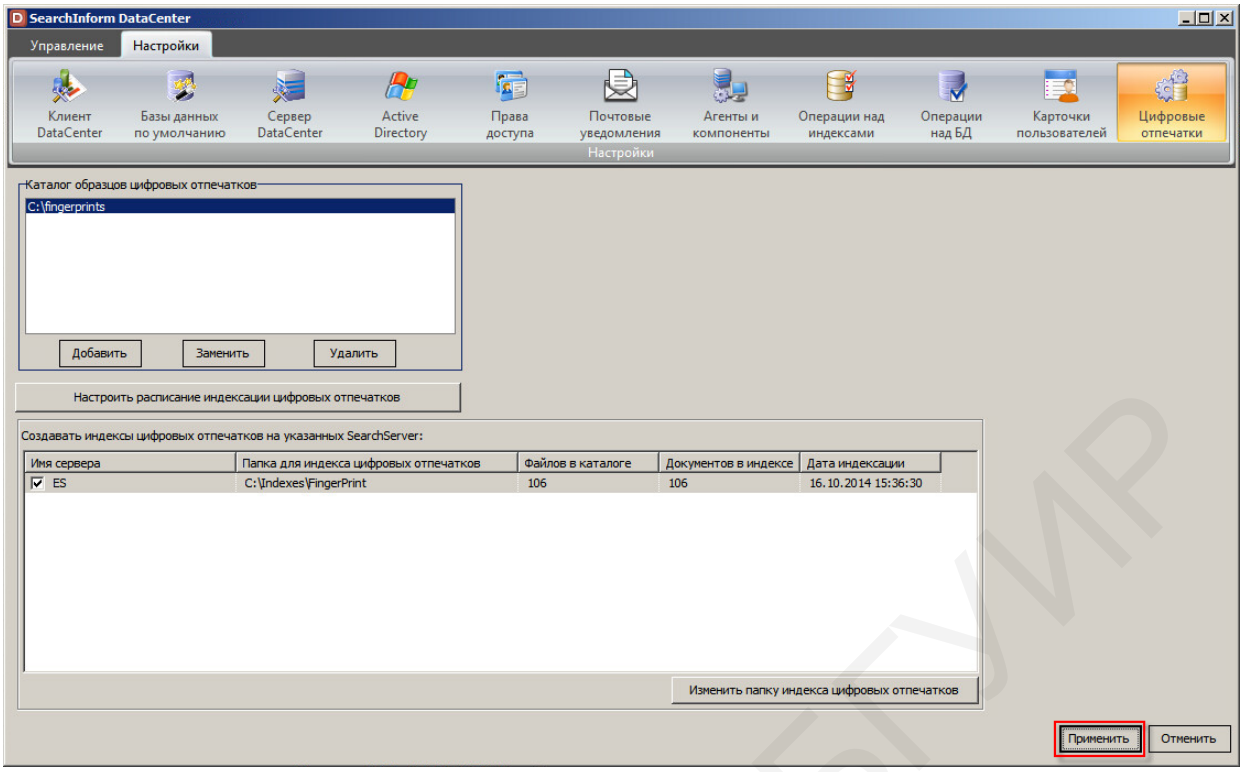


Рис. 2.150. Подтверждение изменений

Библиотека БГУИР

3. ПОИСК, ПРОСМОТР И АНАЛИЗ ПЕРЕХВАЧЕННЫХ ДАННЫХ

3.1. Поиск по перехваченным документам при помощи приложения SearchInform Client

Общая характеристика и ключевые функции SearchInform Client. Программный продукт SearchInform Client входит в состав КИБ и предназначен для отслеживания утечек конфиденциальной информации через электронную почту, Skype, IM-клиенты, FTP-серверы, принтеры, подключаемые внешние устройства, браузерную активность пользователя: блоги, интернет-форумы, файлообменные службы, веб-чаты, веб-формы, социальные сети, браузерные клиенты (ICQ2Go, AIM Express), серверы веб-почты. Клиентское приложение выполняет поиск по перехваченным документам, подключаясь к индексам, расположенным на серверах индексации. Индексы различаются в зависимости от канала передачи данных (Mail, HTTP, Skype и др.).

К ключевым функциям SearchInform Client относятся:

1) мониторинг почтовых сообщений и вложенных файлов, переданных пользователями по протоколам:

– Web mail (Exchange Web Services – исходящая и входящая почта, Kerio Outlook Connect – исходящая и входящая почта, Outlook Web App и Outlook Web Applight – исходящая почта, Zimbra Web Client – исходящая и входящая почта, а также исходящая и входящая корреспонденция с различных почтовых веб-серверов);

– IMAP (в том числе IMAP Compressed);

– MAPI (в том числе RPC over HTTP);

– NNTP;

– POP3;

– SMTP;

2) мониторинг текстового и голосового трафика Skype, включая вложенные файлы и SMS-сообщения;

3) мониторинг HTTP(S)-трафика, отправляемого из браузеров при помощи методов GET и POST;

4) мониторинг сообщений и файлов, переданных пользователями по протоколам:

– OSCAR (ICQ, QIP);

– MSNP (MSN/Windows Live);

– XMPP (Jabber, Google Hangouts);

– MMP (Mail.ru Agent);

– HTTP IM (Facebook, LinkedIn, В Контакте, Мой Мир@Mail.Ru, Одноклассники.ru, Google+, Mamba.ru, Imo.im, Meebo.com);

– SIP (Microsoft Lync, X-lite и др.);

– Gadu-Gadu (Gadu-Gadu);

5) мониторинг информации, передаваемой пользователем на внешние устройства;

6) мониторинг входящего и исходящего FTP-трафика;

7) мониторинг содержимого документов, отправленных пользователем на печать;

8) мониторинг содержимого экранов пользователей;

9) мониторинг разговоров сотрудников;

10) мониторинг текстового и голосового трафика Microsoft Lync, включая вложенные файлы;

11) мониторинг текстового и голосового трафика Viber, включая вложенные файлы;

12) мониторинг активности пользователей в запускаемых ими приложениях в течение рабочего дня;

13) мониторинг журналов безопасности контроллера домена;

14) мониторинг документов, хранящихся на рабочих станциях корпоративной сети;

15) быстрый поиск по тексту перехваченных сообщений и вложенных файлов (полнотекстовый, фразовый поиск, поиск похожих документов);

16) атрибутный поиск по перехваченным сообщениям;

17) просмотр истории переписки с возможностью среза активности по пользователям;

18) фильтрация результатов поиска по заданным атрибутам;

19) экспорт найденных поисковым клиентом документов.

Консоль SearchInform Client используется для формирования запроса, отображения списка результатов и просмотра выделенных документов. Возможна работа как со строкой вкладок, так и в режиме мультиоконности, когда для каждого поискового запроса может быть открыто отдельное окно, которое можно перемещать и масштабировать в рамках главного окна. Характеристика основных элементов интерфейса консоли SearchInform Client представлена в табл. 3.1, внешний вид интерфейса приведен на рис. 3.1.

Таблица 3.1

Основные элементы интерфейса консоли SearchInform Client

Номер элемента на рис. 3.1	**Наименование элемента**	**Назначение**
1	Строка меню	Используется для вызова основных команд настройки консоли. При выборе одной из них пользователь получает доступ к ниспадающему подменю, содержащему перечень входящих в него команд
2	Панель подключения индексов	Используется для подключения к индексам, содержащим информацию по перехваченным документам
3	Панель поиска	Предназначена для формирования запросов
4	Панель результатов	Предназначена для отображения списка результатов поиска
5	Окно предпросмотра	Предназначена для просмотра текущего результата поиска
6	Строка состояния	Отображает общее количество результатов поиска и количество результатов поиска, отображаемых в окне предпросмотра, а также имена операций, выполняемых SearchInform Client

Библиотека БГУИР

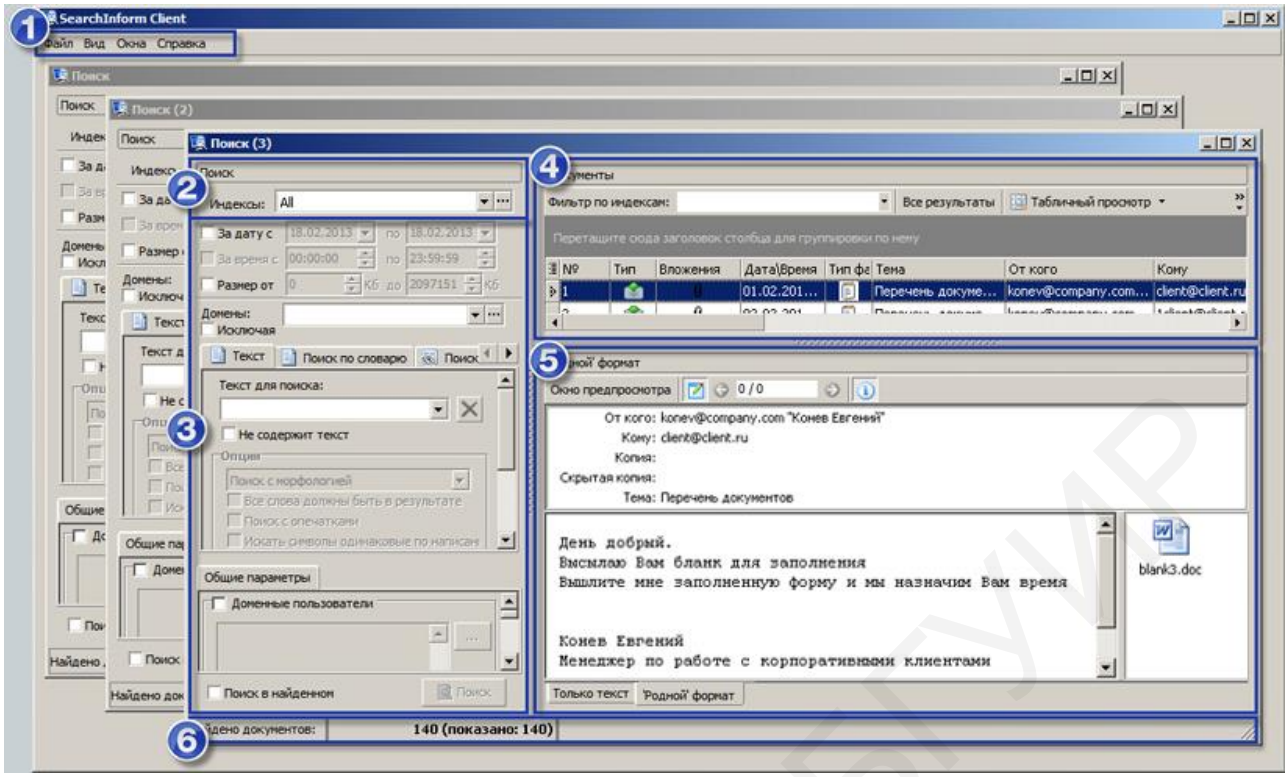


Рис. 3.1. Интерфейс консоли SearchInform Client

SearchInform Client выполняет поиск по перехваченным документам, подключаясь к индексам сервера индексации. Подключение производится на панели подключения индексов – в выпадающем списке «Индексы» необходимо выбрать группу индексов, по которым будет производиться поиск (рис. 3.2).

Если необходимая группа отсутствует, ее можно создать в окне настройки групп индексов, которое вызывается нажатием кнопки ··· в строке «Индексы». Для этого необходимо нажать кнопку «Добавить» и ввести имя новой группы индексов (рис. 3.3).

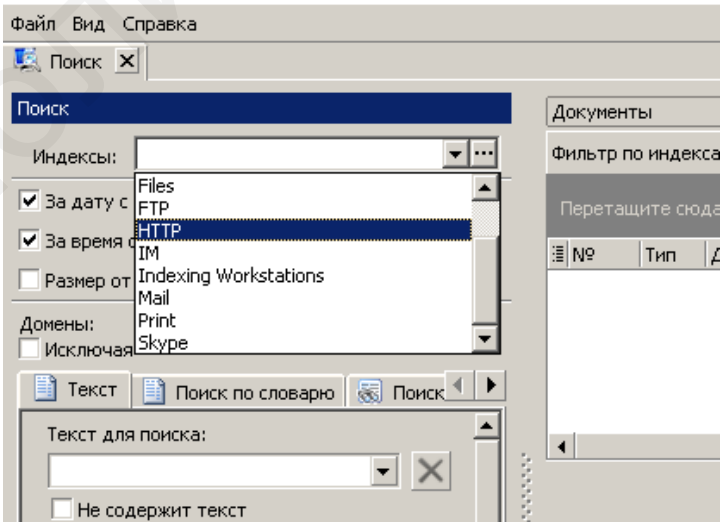


Рис. 3.2. Подключение к индексам сервера индексации

Библиотека БГУИР

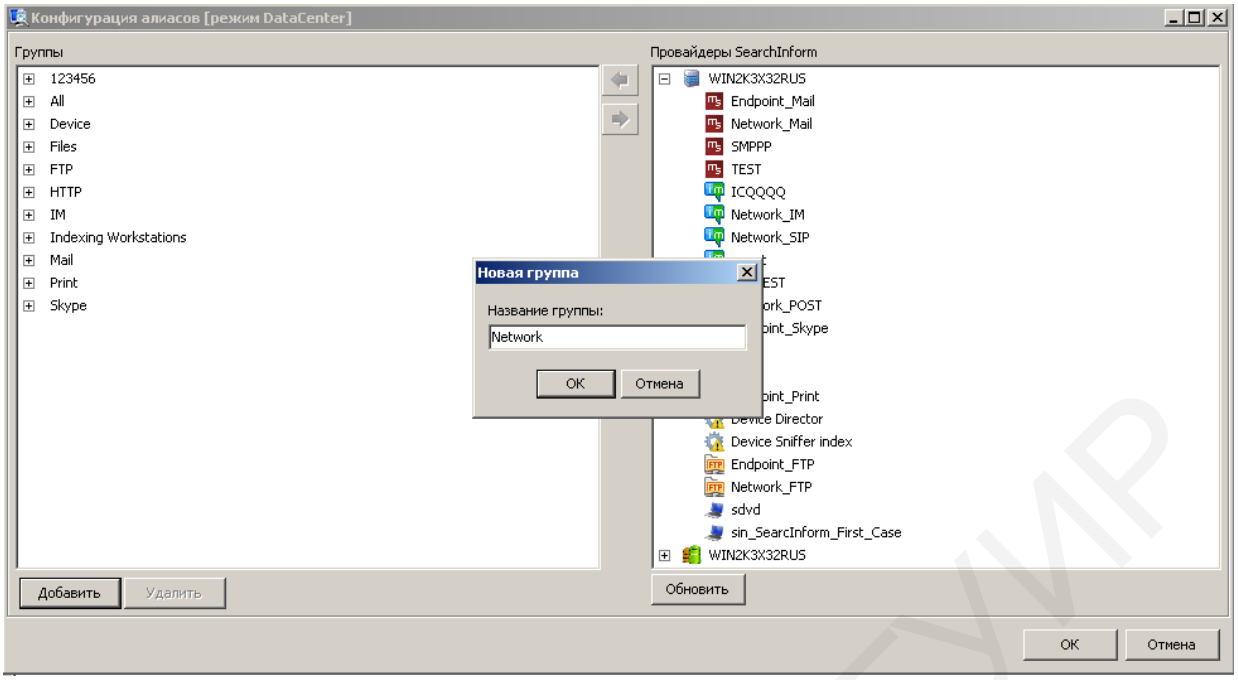


Рис. 3.3. Добавление новой группы индексов

Учетная запись, под которой открыт клиент, должна иметь право доступа к индексам. Если права доступа к серверу индексации нет, следует щелкнуть по имени сервера правой кнопкой мыши и выбрать из контекстного меню команду «Подключиться как», после чего ввести в соответствующем окне необходимые данные.

Для актуализации данных на физических серверах необходимо нажать кнопку «Обновить», с помощью стрелки перенести из правой части окна настройки в левую необходимые серверы и индексы, привязав их к новой группе. Новая группа индексов будет сформирована. Для сохранения произведенных настроек следует воспользоваться кнопкой «OK».

Текстовый поиск. Целью текстового поиска является обнаружение документов, содержащих ключевые слова. SearchInform Client позволяет производить гибкую настройку условий проверки по ключевым словам. Настройки текстового поиска задаются на вкладке «Текст» панели поиска (рис. 3.4). Описание опций для настройки текстового поиска представлено в табл. 3.2. Выбор первых пяти опций таблицы производится с помощью выпадающего списка в одноименном поле.

Для поиска сообщений по ключевому слову или нескольким словам в поле «Текст» необходимо ввести запрос и нажать кнопку «Поиск». Для поиска сообщений, которые не содержат ключевое слово (слова), следует установить флажок в строке «Не содержит текст». Стрелка справа служит для раскрытия выпадающего списка, содержащего историю предыдущих поисковых запросов. Для удаления истории поисковых запросов можно воспользоваться кнопкой  («Очистить историю»).

Библиотека БГУИР

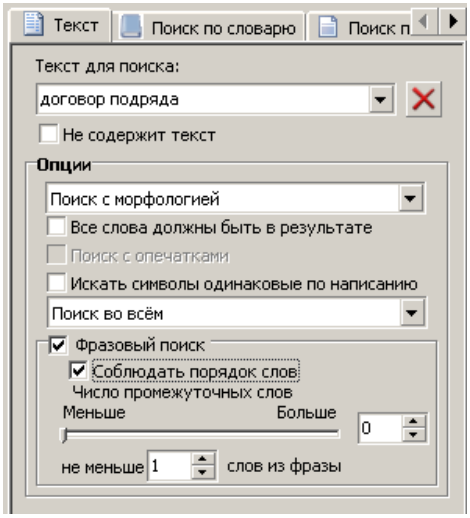


Рис. 3.4. Настройки текстового поиска на вкладке «Текст»

Таблица 3.2

Описание опций для настройки текстового поиска

Наименование опции	**Назначение**
1	**2**
Поиск с морфологией	Благодаря использованию особого аналитического блока могут быть идентифицированы все возможные словоформы. При запросе «автомобиль» производится поиск всех возможных словоформ – «автомобиль», «автомобили», «автомобилей» и т. д.
Точное совпадение	Обнаруживаются только заданные пользователем словоформы. При запросе «автомобиль» будут обнаружены лишь документы, содержащие словоформу «автомобиль»
Начинающиеся со слов	Обнаруживаются словоформы, начинающиеся с заданной пользователем комбинации символов. При запросе «автомобиль», будет идентифицирована как словоформа «автомобиль», так и иные слова начинающиеся с «автомобиль-», например, «автомобильный»
Содержащие слова	Идентифицирует слова, содержащие сочетание символов запроса. Удобно использовать для нахождения документов, содержащих однокоренные слова. При запросе «рабо» идентифицируются такие словоформы, как «работа», «обработка», «работать»
Оканчивающиеся на слова	Поиск всех словоформ, оканчивающихся на заданное пользователем сочетание символов. При запросе «электростанция» обнаруживаются документы, содержащие словоформы «теплоэлектростанция», «гидроэлектростанция»
Все слова должны быть в результате	Установка флажка используется для ограничения результатов поиска документами, содержащими слова запроса
Поиск с опечатками	Установка флажка используется для поиска слов в документе, которые могут отличаться от слов запроса одним или двумя подряд идущими символами. При запросе «молоко» будут идентифицированы словоформы «молако» и «малоко». Написание «малако» идентифицировано не будет, т. к. представляет собой двойную опечатку. При запросе «бит» будут идентифицированы слова «байт», «блат», «болт» и «бот». **Опция «Поиск с опечатками» недоступна при выбранных опциях «Поиск с морфологией» и «Содержащие слова»**

Окончание табл. 3.2

1	2
Искать символы одинаковые по написанию	Установка флажка используется для идентификации слов, в которых использованы совпадающие по написанию буквы русского и латинского алфавитов. Например, при наличии запроса «ABC» идентифицируются все возможные сочетания кириллических и латинских букв
Поиск во всем / Искать во вложениях / Поиск без вложений	Определите, в какой части сообщения искать введенный текст. Поиск может производиться исключительно по вложенным файлам, по тексту самих сообщений, исключая вложения, либо по обоим источникам данных
Фразовый поиск	Представляет собой поиск внутри одного предложения и является частным случаем текстового поиска, при котором можно зафиксировать порядок следования слов и выражений запроса
Соблюдать порядок слов	Представляет собой частный случай фразового поиска, при котором строго учитывается порядок слов
Число промежуточных слов	С помощью ползунка регулируется количество промежуточных слов, которые не учитываются при фразовом поиске

Поиск по словарю. Поиск по тематическим словарям позволяет отыскать документы, относящиеся к определенной тематике. При этом в редактор параметров поиска вводится некоторое количество слов, относящихся к заданной теме (например, теме наркомании, алкоголизма, денежных долгов, компьютерных игр и т. д.), после чего по данному словарю опрашиваются выбранные индексы.

Для осуществления данного вида поиска необходимо:

– перейти на вкладку «Поиск по словарю» панели поиска в главном окне SearchInform Client (рис. 3.5);

– ввести относящиеся к заданной теме слова вручную или вставить их из буфера обмена (также можно вставить готовый набор слов из внешнего .txt-документа, воспользовавшись для этого кнопкой «Вставить словарь из файла»);

– настроить дополнительные параметры поиска (табл. 3.3);

– нажать кнопку «Поиск».

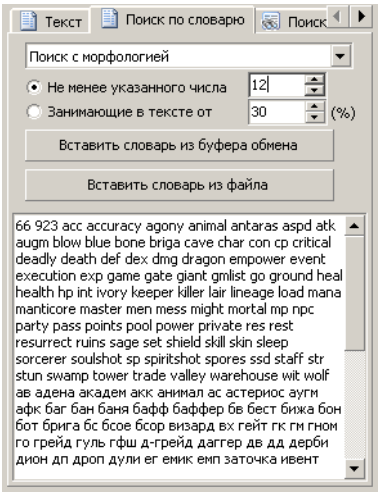


Рис. 3.5. Настройки поиска на вкладке «Поиск по словарю»

Библиотека БГУИР

Таблица 3.3

Описание опций для настройки поиска по словарю

Наименование опции	Назначение
Поиск с морфологией	Благодаря использованию особого аналитического блока могут быть идентифицированы все возможные словоформы. При запросе «автомобиль» производится поиск всех возможных словоформ – «автомобиль», «автомобили», «автомобилей» и т. д.
Точное совпадение	Обнаруживаются только заданные пользователем словоформы. При запросе «автомобиль» будут обнаружены лишь документы, содержащие словоформу «автомобиль»
Не менее указанного числа	В результаты поисковой выдачи попадут только те документы, в которых количество слов из тематического словаря больше или равно указанному числу
Занимающие в тексте от … (%)	В результаты поисковой выдачи попадут только те документы, в которых процент содержания слов из тематического словаря больше или равен указанному числу

При наличии в документе указанного количества слов (или заданного процентного содержания слов) из тематического словаря он будет отображен на панели результатов (рис. 3.6). При поиске по словарю подсветка найденных слов в окне предпросмотра возможна лишь на вкладке «Только текст» (открывается по умолчанию).

Для очистки поискового запроса необходимо щелкнуть правой кнопкой мыши по заголовку вкладки «Поиск по словарю» и выбрать команду «Очистить».

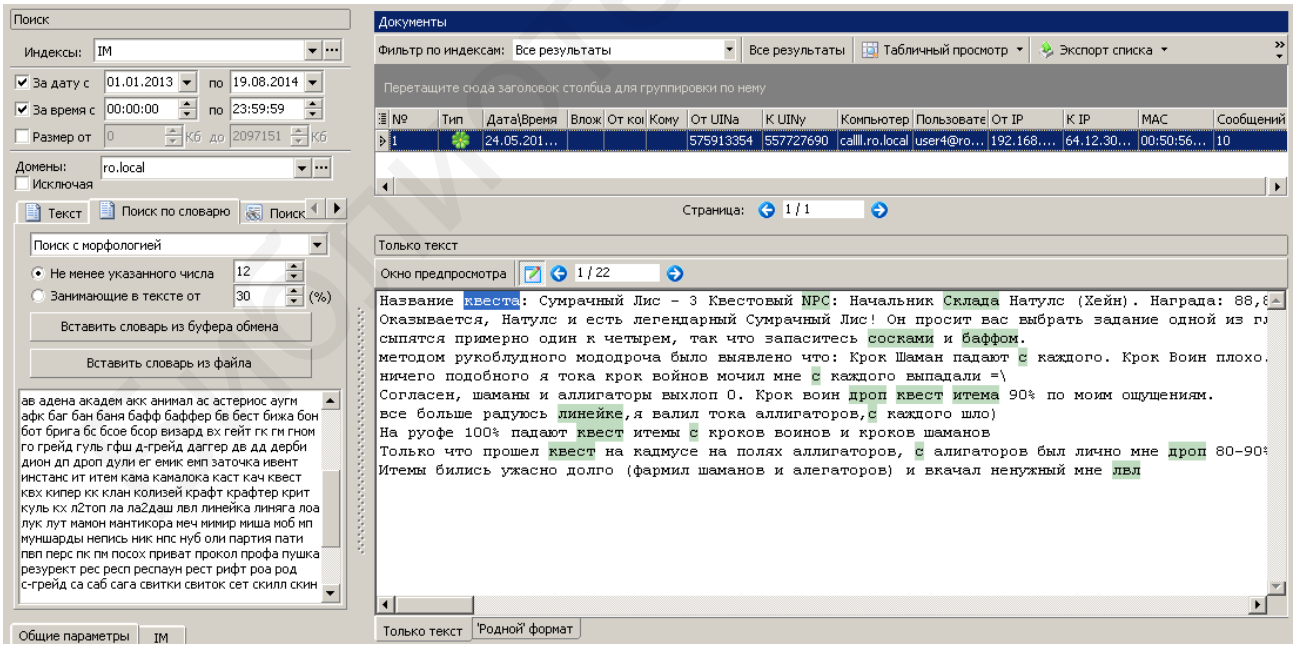


Рис. 3.6. Результаты поисковой выдачи при использовании поиска по словарю

Поиск «похожих». Данный вид поиска основывается на запатентованном алгоритме «Поиск похожих» и позволяет отслеживать конфиденциальные дан-

ные даже в том случае, если текст документа был предварительно отредактирован. В качестве поискового запроса можно использовать как фрагменты текста, так и документы целиком.

Для осуществления данного вида поиска необходимо:

– перейти на вкладку «Поиск похожих» панели поиска в главном окне SearchInform Client (рис. 3.7);

– ввести текст запроса вручную или вставить из буфера обмена (для выполнения операции необходимо ввести не менее 20 символов);

– настроить уровень релевантности (процентного показателя соответствия документа запросу), который может быть задан в пределах 1–100 %, где 1 % – наименьшее возможное соответствие документа условиям поиска, а 100 % – полное совпадение; при снижении показателя требуемой релевантности вероятность обнаружения документов возрастает, при увеличении показателя вероятность обнаружения документов снижается;

– нажать кнопку «Поиск».

Список обнаруженных документов отобразится на панели результатов.

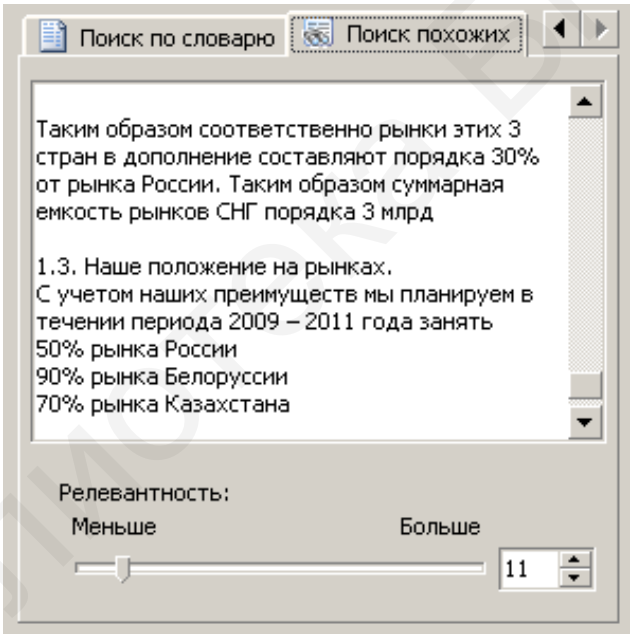


Рис. 3.7. Настройки поиска на вкладке «Поиск похожих»

Для очистки поискового запроса необходимо щелкнуть правой кнопкой мыши по заголовку вкладки «Поиск похожих» и выбрать команду «Очистить».

Поиск похожих можно производить по тексту целого документа. Для этого необходимо выбрать документ из списка результатов и нажать кнопку «Поиск похожих» на панели результатов или выбрать команду «Поиск похожих» в контекстном меню (рис. 3.8). Для последующего поиска среди уже имеющихся результатов в левом нижнем углу панели поиска следует установить флажок в строке «Поиск в найденном» (при получении в результатах поиска слишком большого числа документов рекомендуется выполнить повторный поиск, применив ограничения к уже выведенным результатам).

Библиотека БГУИР

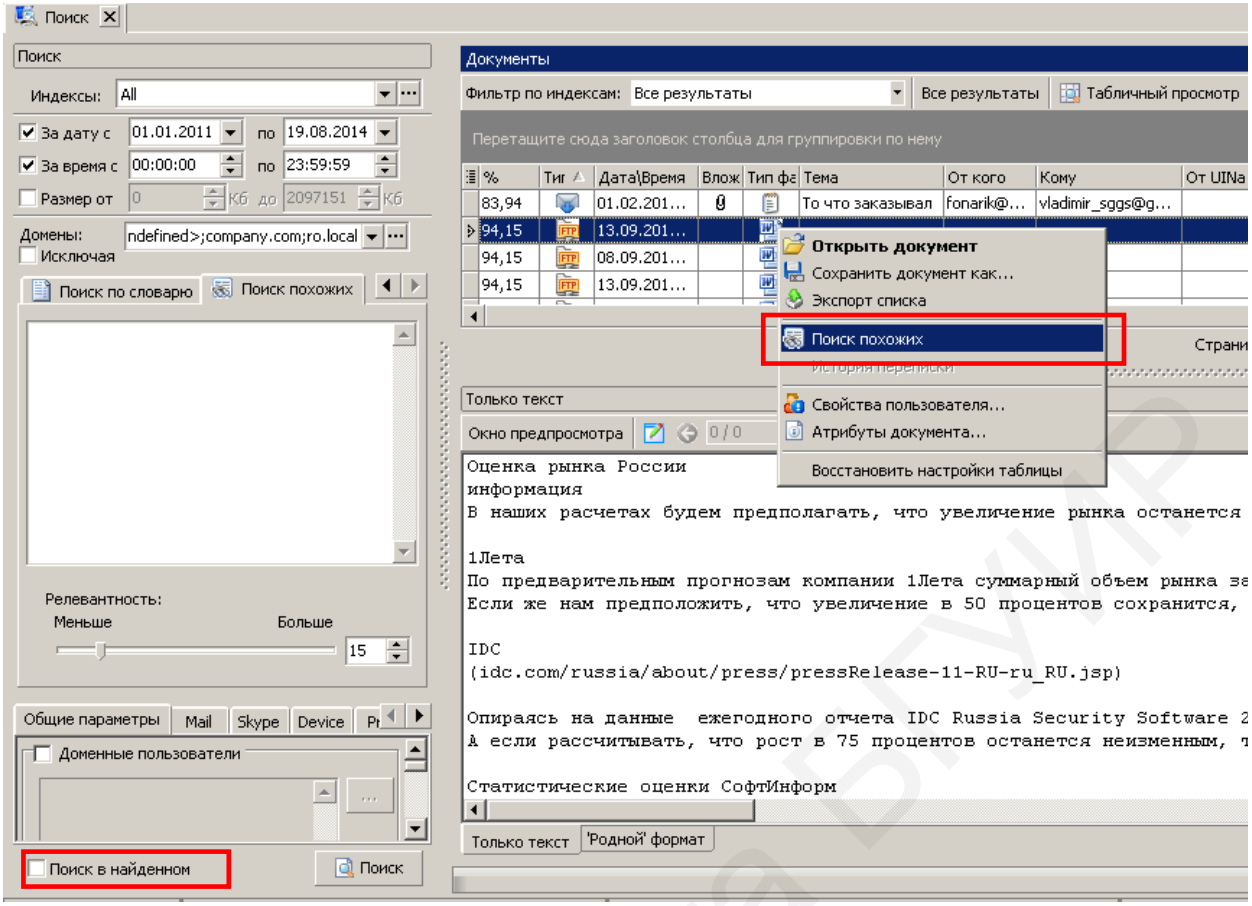


Рис. 3.8. Поиск «похожих» по тексту целого документа

Для просмотра всех перехваченных сообщений необходимо подключить индексы и, не вводя запрос в поле «Текст для поиска» и не указывая каких-либо других ограничений, нажать кнопку «Поиск», расположенную в нижней части главного окна (рис. 3.9).

Ограничение результатов поиска. Поиск документов можно ограничивать по следующим общим параметрам: дате перехвата, времени перехвата, размеру документа, доменным пользователям, использованию SSL и другим общим атрибутам.

Для ограничения результатов поиска по дате (рис. 3.10) следует:

– установить флажок в строке «За дату с»;

– воспользоваться календарем для настройки начальной и конечной даты либо ввести требуемые даты вручную;

– нажать кнопку «Пуск» для начала поиска либо перейти к выбору других ограничений.

Для ограничения результатов поиска по времени (рис. 3.10) необходимо:

– установить флажок в строке «За время с»;

– ввести начальное и конечное время, которым должен быть ограничен поиск перехваченных документов;

– нажать кнопку «Поиск» для начала поиска либо перейти к выбору других ограничений.

Библиотека БГУИР

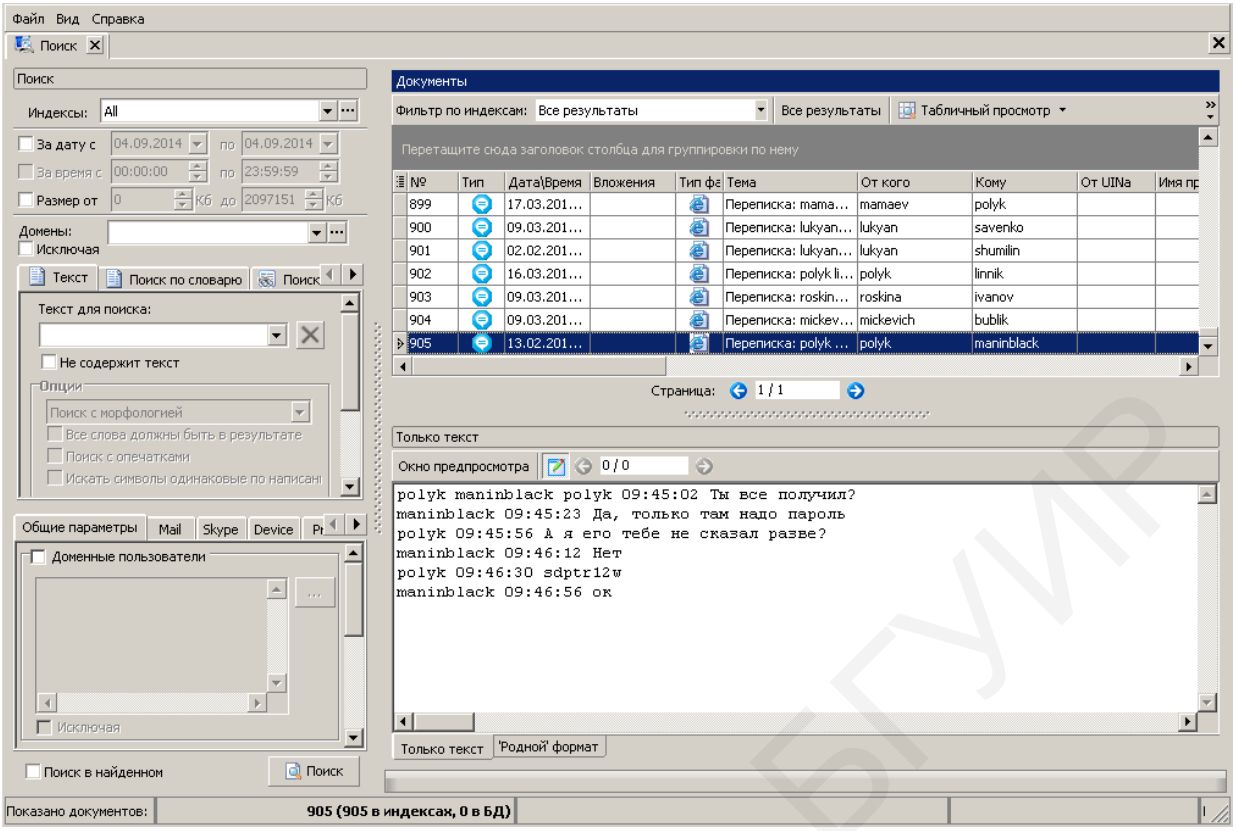


Рис. 3.9. Просмотр всех перехваченных сообщений

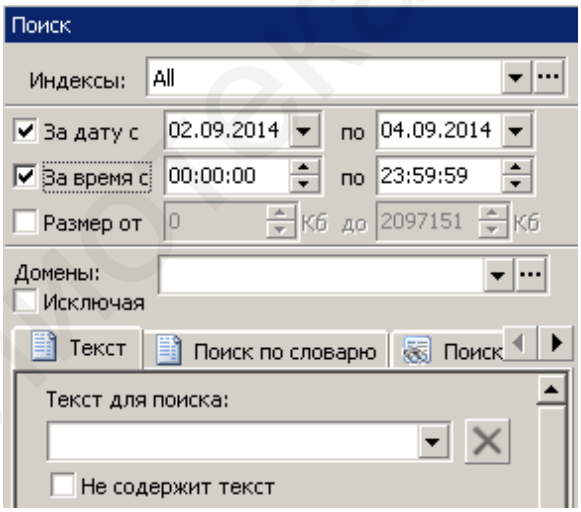


Рис. 3.10. Ограничение результатов поиска по дате и времени

Для ограничения результатов поиска по размеру (рис. 3.11) необходимо:

– установить флажок в строке «Размер от»;

– ввести диапазон размера, который могут иметь перехваченные файлы;

– нажать кнопку «Поиск» для начала поиска либо перейти к выбору других ограничений.

Для ограничения результатов поиска по домену (см. рис. 3.11) следует:

– в поле «Домены» ввести домен, который будет включен/исключен из поиска (для исключения домена из поиска следует установить флажок в строке «Исключая»);

Библиотека БГУИР

– нажать кнопку «Пуск» для начала поиска либо перейти к выбору других ограничений.

Выбор домена также можно произвести путем вызова соответствующего списка при помощи кнопки ··· (рис. 3.12).

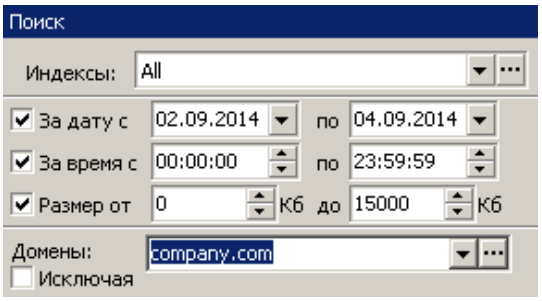


Рис. 3.11. Ограничение результатов поиска по размеру и домену

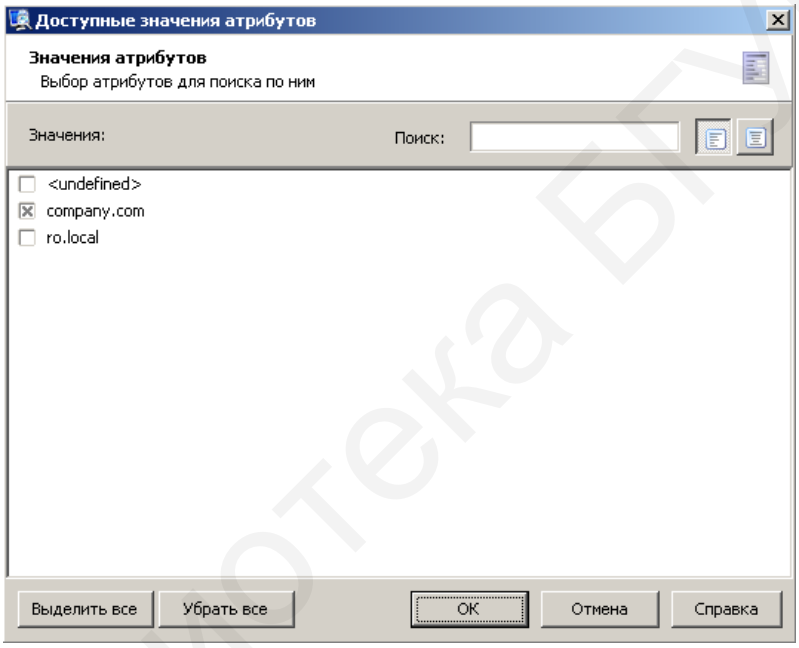


Рис. 3.12. Выбор домена для ограничения результатов поиска

Ограничение результатов поиска по доменным пользователям производится в нижней части панели поиска на вкладке «Общие параметры» (рис. 3.13). Для этого следует:

– установить флажок в строке «Доменные пользователи»;

– ввести список пользователей, по которым будет производиться поиск, вручную либо при помощи кнопки ··· для выбора пользователей из списка;

– для исключения документов добавленных пользователей из списка результатов установить флажок в строке «Исключая»;

– нажать кнопку «Поиск» для начала поиска либо перейти к выбору других ограничений.

Библиотека БГУИР

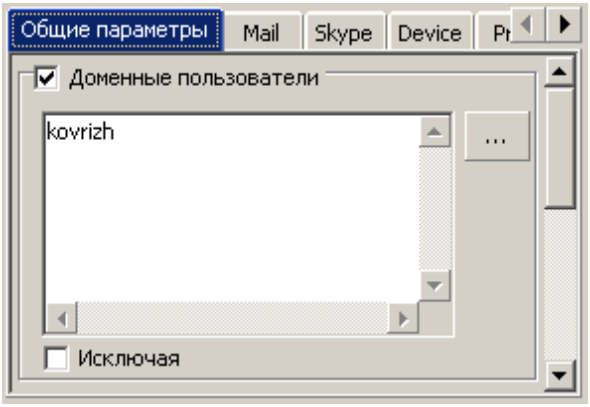


Рис. 3.13. Ограничение результатов поиска по доменным пользователям

Для исключения из результатов поиска документов, при передаче которых использовалось безопасное соединение (протокол SSL), необходимо:

– установить флажок в строке «SSL» в нижней части панели поиска (рис. 3.14);

– активировать переключатель «Исключая» (при выборе опции «Включая» поиск будет производиться по всем данным, в том числе и тем, которые передавались по SSL-протоколу);

– нажать кнопку «Поиск» для начала поиска либо перейти к выбору других ограничений.

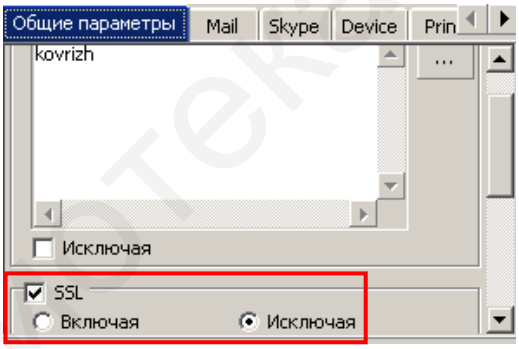


Рис. 3.14. Исключение из результатов поиска документов,
при передаче которых использовалось безопасное соединение (протокол SSL)

Ограничение поиска по именам компьютеров, IP/MAC-адресам, именам и типам файлов производится в нижней части панели поиска на вкладке «Общие параметры» (рис. 3.15). При помощи выпадающего списка «Объединение параметров поиска» различные параметры поиска могут либо обрабатываться отдельно, либо объединяться. Для этого используется одна из двух возможных позиций:

– «Логическое ИЛИ» – каждый из параметров поиска обрабатывается отдельно, безотносительно к другим параметрам;

– «Логическое И» – различные параметры поиска объединяются и обрабатываются как единое целое.

Для настройки ограничения поиска по именам компьютеров, IP/MAC-адресам, именам и типам файлов необходимо:

Библиотека БГУИР

– установить флажок напротив соответствующего параметра;

– ввести список значений атрибута, по которым будет производиться поиск, вручную либо при помощи кнопки ... для выбора из списка;

– если результаты поиска не должны удовлетворять указанному значению атрибута, выбрать в первом выпадающем списке напротив параметра значение «Not» (документы, значения атрибутов которых совпадают с указанными, могут либо включаться в поисковую выдачу, либо исключаться, значением по умолчанию является «включено» (пустое значение));

– для строковых атрибутов (например, «Компьютер») поддерживается использование модификаторов (см. ниже), включающих специфический режим обработки поискового запроса;

– нажать кнопку «Поиск» для начала поиска либо перейти к выбору других ограничений.

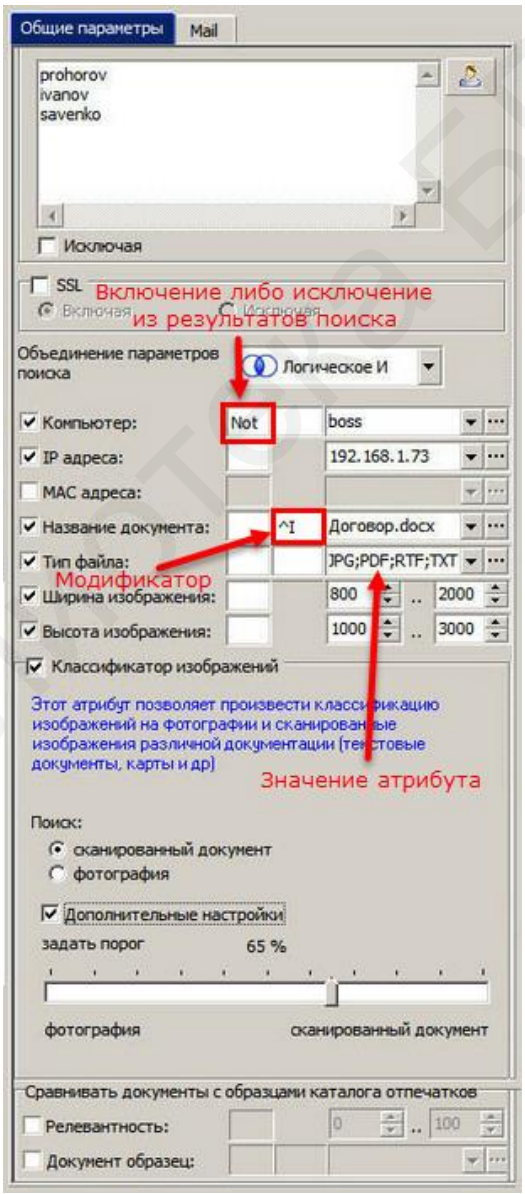


Рис. 3.15. Ограничение поиска по именам компьютеров, IP/MAC-адресам и другим общим атрибутам

Библиотека БГУИР

Использование модификаторов. Под модификатором понимается набор символов, который вводится в строке поиска непосредственно перед выражением поискового запроса. Наличие в строке поиска модификатора включает специфический режим обработки поискового запроса. Например, режим поиска подстроки с учетом регистра, режим поиска подстроки без учета регистра, режим поиска с полным совпадением строки и т. п. Модификаторы используются при поиске по атрибутам (адрес электронной почты, тема письма, имя компьютера, доменное имя пользователя и т. д.) независимо от типа подключенного индекса: Mail, Print, HTTP, IM и пр. Модификаторы поиска можно выбирать из выпадающих списков как общие для всех значений, а также переопределять вручную для каждого значения атрибута в отдельности. Перечень используемых в SearchInform Client модификаторов представлен в табл. 3.4.

Таблица 3.4

Модификаторы

Модификатор	**Назначение**	**Пример использования**
^S	Применение поиска подстроки с учетом регистра	При вводе имени компьютера ^SDemchenko будет возможным нахождение имен Demchenko, IvanDemchenko, Demchenko-PC, но такие имена компьютера, как DEMCHENKO, DEMCHENKO-PC, DemchenKO, Demchen-ko, в результаты поиска не попадут
^I	Применение поиска подстроки без учета регистра	При вводе имени компьютера ^IDemchenko будет возможным нахождение имен Demchenko, IvanDemchenko, Demchenko-PC, DEMCHENKO, DEMCHENKO-PC, DemchenKO, в то время как такое имя компьютера, как Demchen-ko , в результаты поиска не попадет
=S	Применение поиска с полным совпадением строки с учетом регистра	При вводе имени компьютера =SDemchenko будет возможным нахождение только имени Demchenko, а такие имена компьютера, как IvanDemchenko, Demchenko-PC, DEMCHENKO, DEMCHENKO-PC, DemchenKO, Demchen-ko, в результаты поиска не попадут
=I	Применение поиска с полным совпадением строки без учета регистра	При вводе имени компьютера =IDemchenko будет возможным нахождение имен Demchenko, DEMCHENKO, DemchenKO, в то время как такие имена компьютера, как IvanDemchenko, Demchenko-PC, DEMCHENKO-PC, Demchen-ko, в результаты поиска не попадут

Библиотека БГУИР

Ограничение поиска по атрибутам. Поиск можно ограничивать по различным атрибутам документа: протоколу, имени компьютера, дате отправки, IP-адресу и т. п. Набор атрибутов зависит от типа подключенного индекса: Mail, HTTP, Skype, IM и др.

Ограничение по атрибутам производится на панели поиска, на вкладках поиска по атрибутам документа – Mail, HTTP, Skype, Device, Print, IM, FTP, Workstation, Monitor, Microphone, Cloud, Lync, Viber. Значения атрибутов вводятся вручную либо выбираются из предложенного списка с помощью кнопки ···. При выборе хотя бы одного атрибута на вкладке ее название будет подсвечиваться.

При выполнении поиска атрибуты могут объединяться, выступая как единое целое, либо обрабатываться отдельно, безотносительно друг к другу. Настройка производится в выпадающем списке «Объединение параметров поиска», включающем две позиции:

– «Логическое ИЛИ» – каждый из параметров поиска по атрибутам документа обрабатывается отдельно, безотносительно к другим параметрам;

– «Логическое И» – различные параметры поиска по атрибутам документа объединяются и обрабатываются как единое целое.

Ограничения по атрибутам сообщений электронной почты настраиваются на вкладке «Mail» (рис. 3.16).

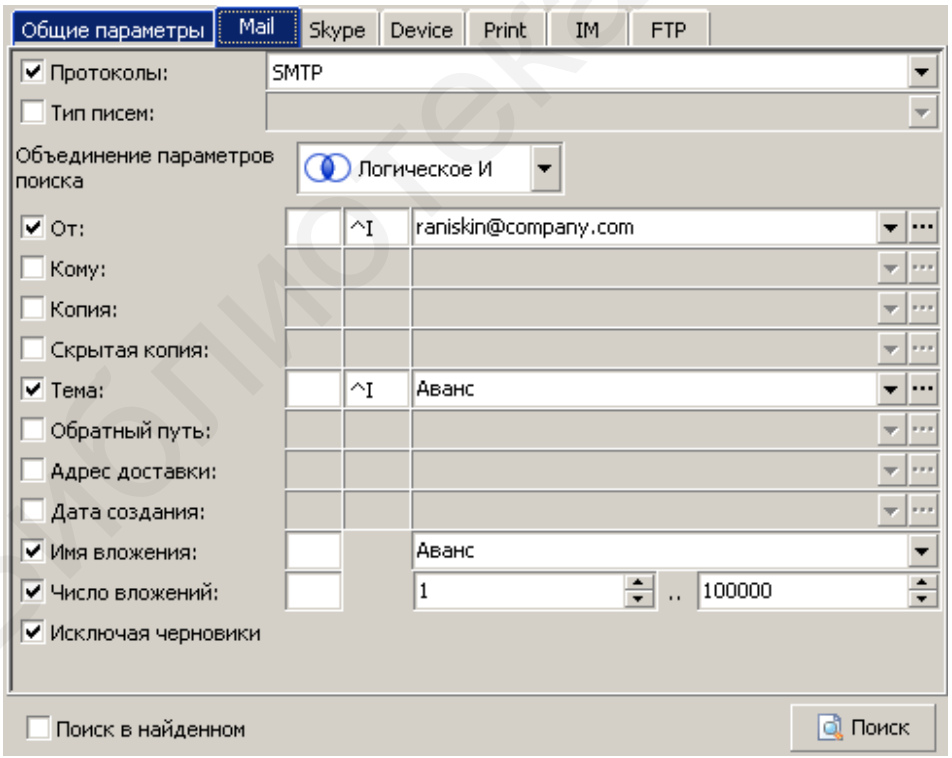


Рис. 3.16. Ограничение поиска по атрибутам сообщений электронной почты

Документы, значения атрибутов которых совпадают с указанными, могут как включаться в поисковую выдачу, так и исключаться. Значением по умолчанию является «включено» (пустое значение). Если результаты поиска

не должны удовлетворять указанному значению атрибута, в первом выпадающем списке напротив параметра требуется выбрать значение «Not».

Для строковых атрибутов поддерживается использование модификаторов, включающих специфический режим обработки поискового запроса.

Назначение используемых атрибутов указано в табл. 3.5.

Таблица 3.5

Атрибуты сообщений электронной почты, по которым возможно ограничение поиска

Атрибут	**Назначение**
Протоколы	Выбор одного или нескольких протоколов, с помощью которых производилась отправка/получение почтовой корреспонденции: IMAP, MAPI, POP3, SMTP, HTTP, NNTP. Для выбора необходимо установить флажок. Если не выбран ни один протокол, поиск будет произведен с настройками по умолчанию – по сообщениям всех протоколов
Тип писем	Определение направления движения электронного сообщения (исходящее/входящее) наряду с возможными протоколами передачи данных
От	Адрес электронной почты отправителя
Кому	Адрес электронной почты получателя
Копия	Адрес(-а) электронной почты получателей копий (CC)
Скрытая копия	Адрес(-а) электронной почты получателей слепых копий (BCC)
Тема	Тема почтового сообщения
Обратный путь	Адрес для ответа на сообщение (Return-path)
Адрес доставки	Оригинальный адрес получателя, основанный на свойствах SMTP (X-Envelope-To)
Дата	Дата отправки сообщения
Имя вложения	Имя файла, вложенного в почтовое сообщение
Число вложений	Количество вложенных в сообщение файлов
Исключая черновики	Включение или исключение из поисковой выдачи черновых вариантов писем (на панели результатов маркируется серым цветом)

Ограничения по атрибутам сообщений, переданных по протоколу HTTP(S), настраиваются на вкладке «HTTP» (рис. 3.17). Документы, значения атрибутов которых совпадают с указанными, могут как включаться в поисковую выдачу, так и исключаться. Значение по умолчанию – «включено» (пустое значение). Если результаты поиска не должны удовлетворять указанному значению атрибута, в первом выпадающем списке напротив параметра требуется выбрать значение «Not».

Для строковых атрибутов поддерживается использование модификаторов. Назначение используемых атрибутов указано в табл. 3.6.

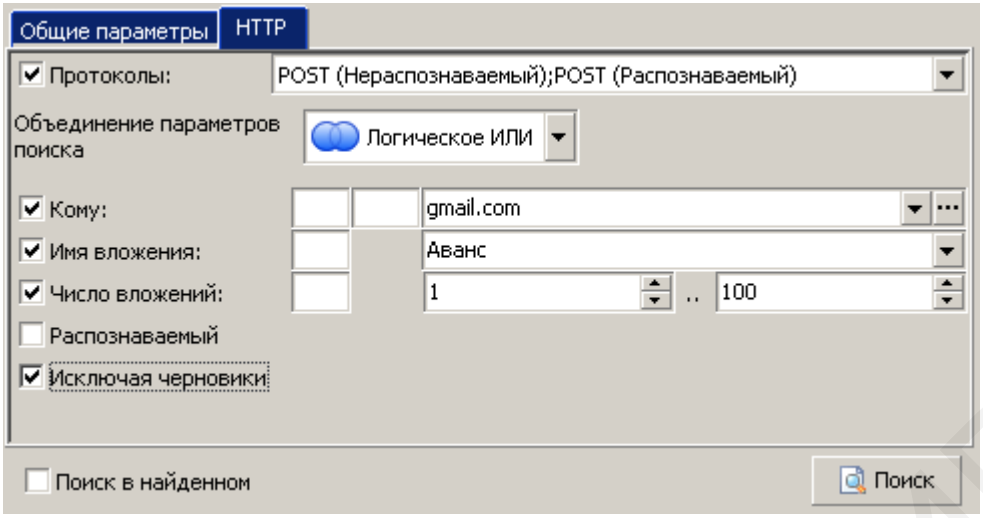


Рис. 3.17. Ограничение поиска по атрибутам сообщений, переданных по протоколу HTTP(S)

Таблица 3.6

Атрибуты сообщений, переданных по протоколу HTTP(S), по которым возможно ограничение поиска

Атрибут	**Назначение**
Протоколы	Выбор метода передачи данных (для выбора необходимо установить флажок): – GET (Нераспознаваемый); – POST (Нераспознаваемый); – GET (Распознаваемый); – POST (Распознаваемый). Если не выбран ни один метод передачи, поиск будет произведен с настройками по умолчанию – по всем документам независимо от метода передачи и набора символов
Кому	Доменные имена посещенных интернет-узлов
Имя вложения	Имя файла, прикрепленного к сообщению
Число вложений	Количество прикрепленных к сообщению файлов
Распознаваемый	Параметр позволяет очистить поисковую выдачу перехваченных POST-запросов от нежелательных символов, не несущих смыслового значения
Исключая черновики	Включение или исключение из поисковой выдачи черновых вариантов сообщений (на панели результатов маркируется серым цветом)

Ограничения по атрибутам Skype-сообщений настраиваются на вкладке «Skype» (рис. 3.18). Документы, значения атрибутов которых совпадают с указанными, могут как включаться в поисковую выдачу, так и исключаться. Значение по умолчанию – «включено» (пустое значение). Если результаты поиска не должны удовлетворять указанному значению атрибута, в первом выпадающем списке напротив параметра требуется выбрать значение «Not».

Для строковых атрибутов поддерживается использование модификаторов. Назначение используемых атрибутов указано в табл. 3.7.

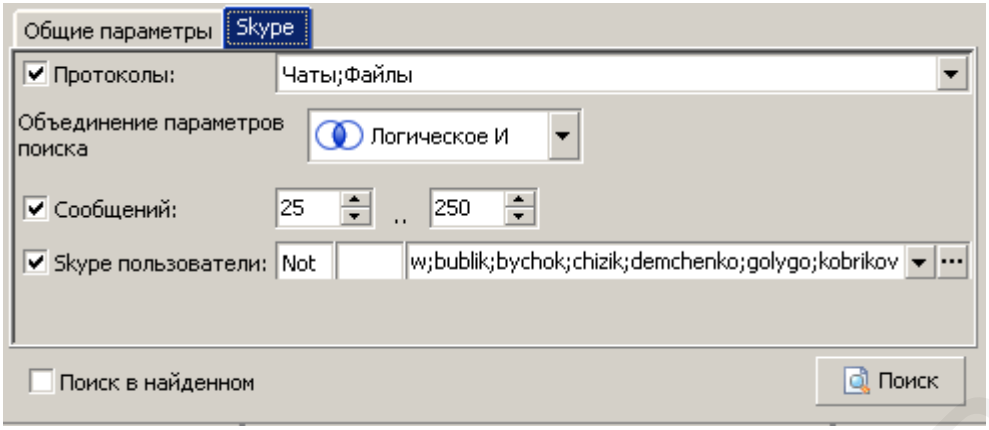


Рис. 3.18. Ограничение поиска по атрибутам Skype-сообщений

Таблица 3.7

Атрибуты Skype-сообщений, по которым возможно ограничение поиска

Атрибут	Назначение
Протоколы	Выбор типа перехваченого документа: чаты, SMS, звонки, файлы. Для выбора следует установить флажок. Если не выбран ни один тип документа, поиск будет произведен с настройками по умолчанию – по всем типам документов
Сообщений	Количество сообщений между пользователями Skype
Skype пользователи	Идентификатор пользователя Skype

Ограничения по атрибутам подключаемых внешних устройств, на которые сохранялись документы, настраиваются на вкладке «Device» (рис. 3.19). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам подключенных индексов. Назначение используемых атрибутов указано в табл. 3.8.

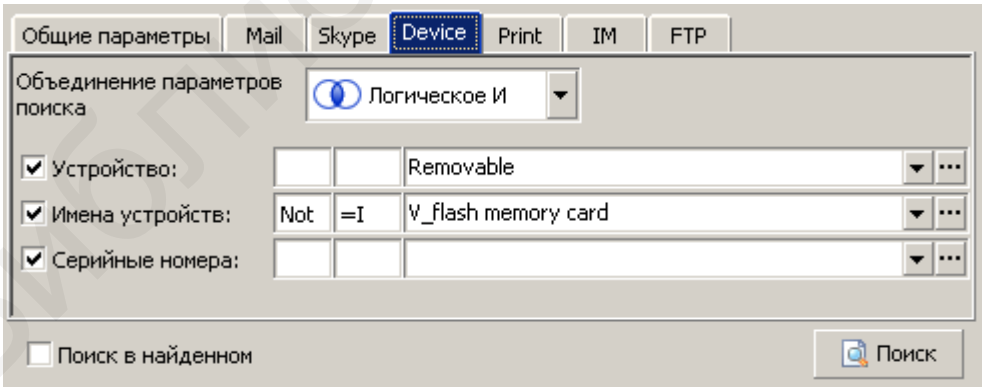


Рис. 3.19. Ограничение поиска по атрибутам подключаемых внешних устройств

Библиотека БГУИР

Таблица 3.8

Атрибуты подключаемых внешних устройств,
по которым возможно ограничение поиска

Атрибут	Назначение
Устройство	Тип внешнего устройства
Имена устройств	Заданное производителем или пользователем имя подключаемого внешнего устройства
Серийные номера	Уникальный номер устройства, присвоенный производителем при изготовлении

Ограничения по атрибутам отправленных на принтер документов настраиваются на вкладке «Print» (рис. 3.20). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам подключенных индексов. Назначение используемых атрибутов указано в табл. 3.9.

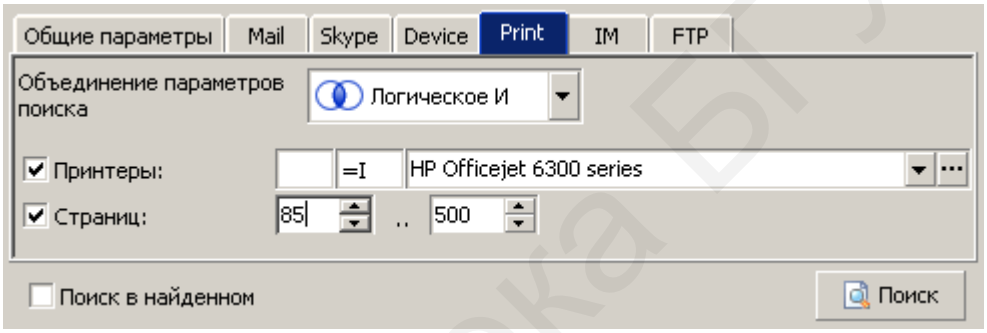


Рис. 3.20. Ограничение поиска по атрибутам отправленных на принтер документов

Таблица 3.9

Атрибуты отправленных на принтер документов, по которым возможно ограничение поиска

Атрибут	Назначение
Принтеры	Имя принтера, на который было отправлено задание печати
Страниц	Количество страниц распечатанного документа

Ограничения по атрибутам передаваемых с помощью IM-клиентов сообщений и файлов настраиваются на вкладке «IM» (рис. 3.21). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам подключенных индексов. Назначение используемых атрибутов указано в табл. 3.10.

Библиотека БГУИР

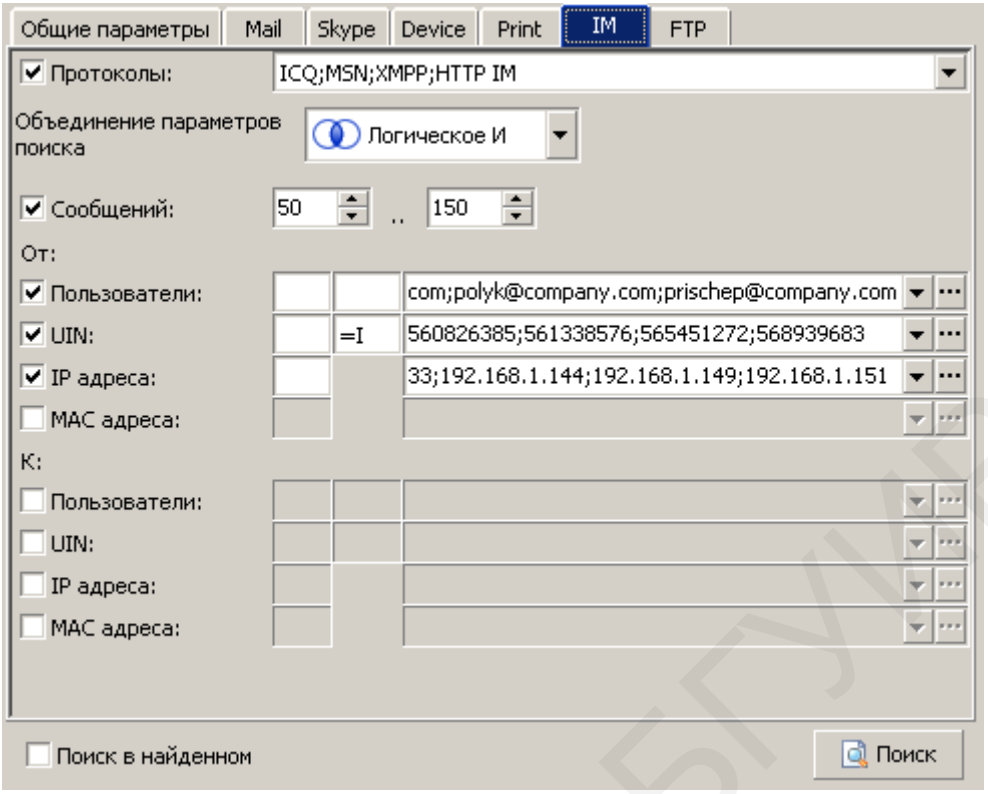


Рис. 3.21. Ограничение поиска по атрибутам передаваемых с помощью IM-клиентов сообщений и файлов

Таблица 3.10

Атрибуты передаваемых с помощью IM-клиентов сообщений и файлов, по которым возможно ограничение поиска

Атрибут	**Назначение**
Протоколы	Выбор одного или нескольких протоколов, с помощью которых производилась отправка/получение сообщений и файлов: ICQ, MSN, MMP, XMPP, HTTP IM, SIP, Gadu-Gadu. Для выбора необходимо установить флажок. Если не выбран ни один протокол, поиск будет произведен с настройками по умолчанию – по сообщениям всех протоколов
Сообщений	Количество сообщений между IM-пользователями
От/к пользователям	Доменное имя пользователя, отправившего/получившего сообщение/файл посредством IM-клиента
От/к UIN	Уникальный идентификатор пользователя, отправившего/получившего сообщение/файл посредством IM-клиента
От/к IP-адресу	IP-адрес пользователя, принявшего/отправившего сообщение/файл
От/к MAC-адресу	MAC-адрес пользователя, принявшего/отправившего сообщение/файл

Ограничения по атрибутам FTP-соединений настраиваются на вкладке «FTP» (рис. 3.22). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам подключенных индексов. Назначение используемых атрибутов указано в табл. 3.11.

Библиотека БГУИР

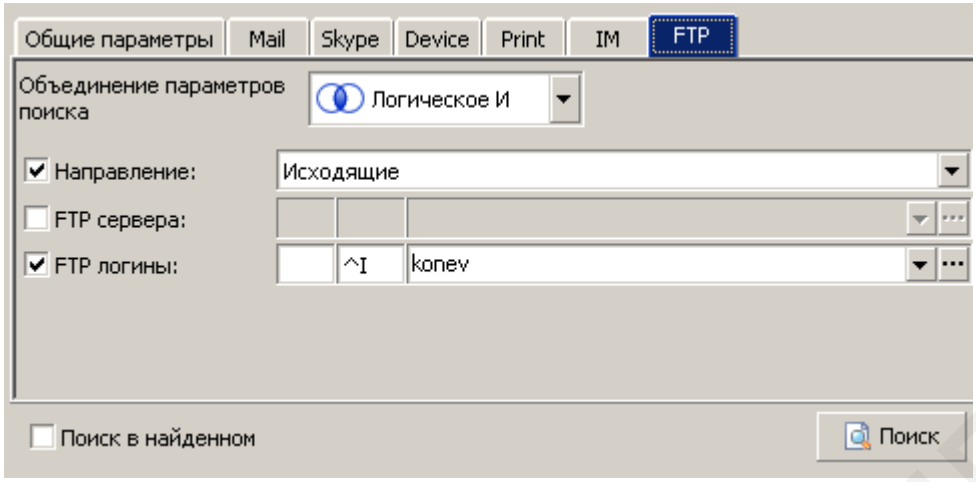


Рис. 3.22. Ограничение поиска по атрибутам FTP-соединений

Таблица 3.11

Атрибуты FTP-соединений, по которым возможно ограничение поиска

Атрибут	Назначение
Направление	Определение направления движения документа (загрузка на сервер FTP или с него)
FTP сервера	Адрес сервера FTP
FTP логины	Идентификатор, используемый для подключения к серверу FTP

Ограничения по атрибутам входящих и исходящих данных облачных сервисов настраиваются на вкладке «Cloud» (рис. 3.23). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам подключенных индексов. Назначение используемых атрибутов указано в табл. 3.12.

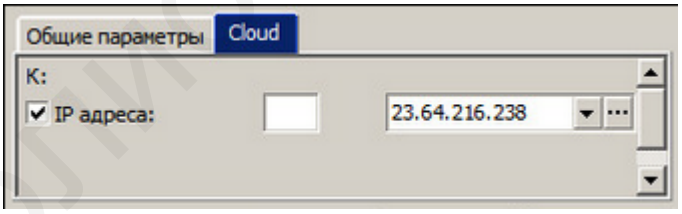


Рис. 3.23. Ограничение поиска по атрибутам облачных сервисов

Таблица 3.12

Атрибуты облачных сервисов

Атрибут	Назначение
(K) IP адреса	IP-адрес облачного хранилища данных, на который загружался либо с которого скачивался документ

Ограничения по атрибутам Viber-сообщений настраиваются на вкладке «Viber» (рис. 3.24). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам. Назначение используемых атрибутов указано в табл. 3.13.

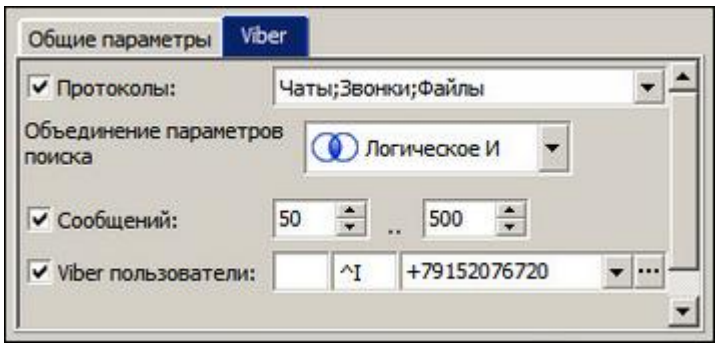


Рис. 3.24. Ограничение поиска по атрибутам Viber-сообщений

Таблица 3.13

Атрибуты Viber-сообщений

Атрибут	Назначение
Протоколы	Выбор типа перехваченого документа: чаты, звонки, файлы. Для выбора установите флажок. Если не выбран ни один тип документа, поиск будет произведен с настройками по умолчанию – по всем типам документов
Сообщений	Количество сообщений между пользователями Viber
Viber пользователи	Мобильные номера пользователей Viber

Настройка ограничения результатов выдачи файловых операций осуществляется на вкладке «User files» (рис. 3.25). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам. Назначение используемых атрибутов указано в табл. 3.14.

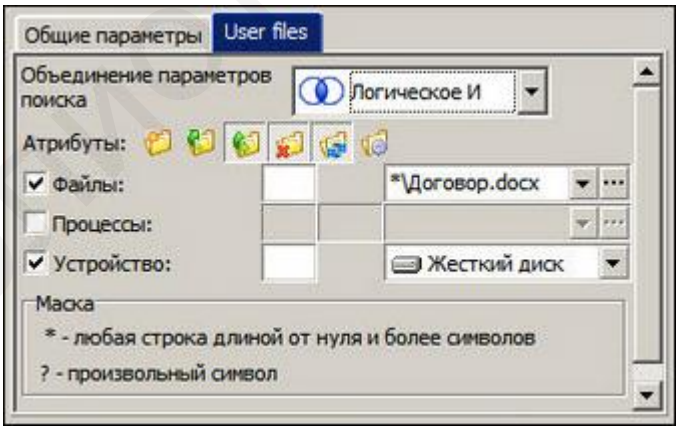


Рис. 3.25. Ограничение поиска по файловых операциям

Таблица 3.14

Атрибуты файловых операций

Атрибут	Назначение
Атрибуты	Типы произведенной файловой операции
Файлы	Путь и имя документа, с которым осуществлялись файловые операции
Процессы	Путь к исполнимому файлу приложения, из которого производились операции с документом
Устройство	Тип устройства, на котором хранился целевой документ

Библиотека БГУИР

Настройка ограничения результатов выдачи записей голосов осуществляется на вкладке «Mic» (рис. 3.26). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам. Назначение используемых атрибутов указано в табл. 3.15.

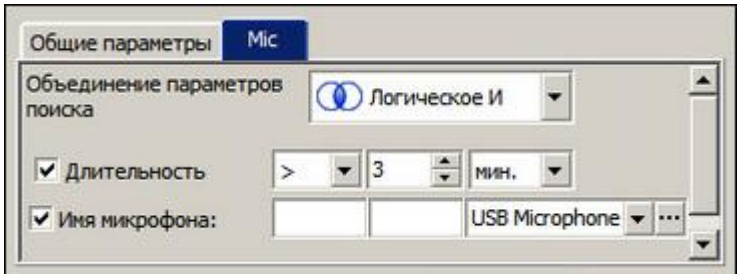


Рис. 3.26. Ограничение поиска по записям микрофона

Таблица 3.15

Атрибуты записей микрофона

Атрибут	Назначение
Длительность	Продолжительность звукового файла
Имя микрофона	Название устройства записи

Настройка ограничения результатов выдачи данных, вводимых пользователем с клавиатуры, осуществляется на вкладке «Keylogger» (рис. 3.27). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам. Назначение используемых атрибутов указано в табл. 3.16.

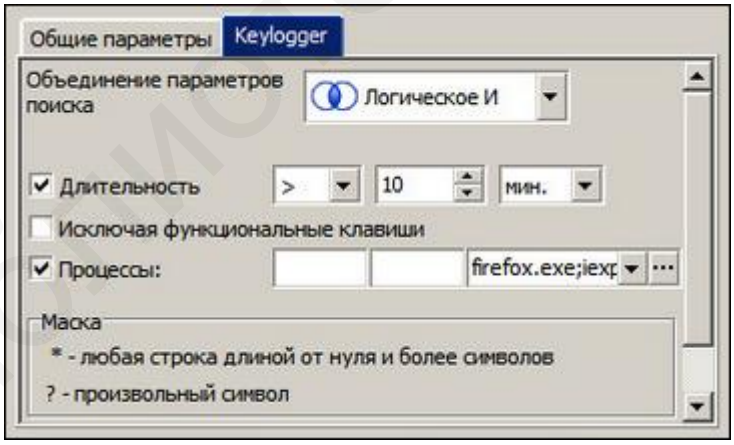


Рис. 3.27. Ограничение поиска по данным Keylogger

Таблица 3.16

Атрибуты перехваченных нажатий клавиш

Атрибут	Назначение
Длительность	Продолжительность времени, проведенного в приложении
Исключая функциональные клавиши	Включение или исключение из выдачи данных с зафиксированными нажатиями системных клавиш (Enter, Esc, F1 и пр.)
Процессы	Исполнимый файл приложения, в котором производилось логирование нажатых клавиш

Библиотека БГУИР

Настройка ограничения результатов выдачи снимков экрана осуществляется на вкладке «Monitor» (рис. 3.28). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам. Назначение используемых атрибутов указано в табл. 3.17.

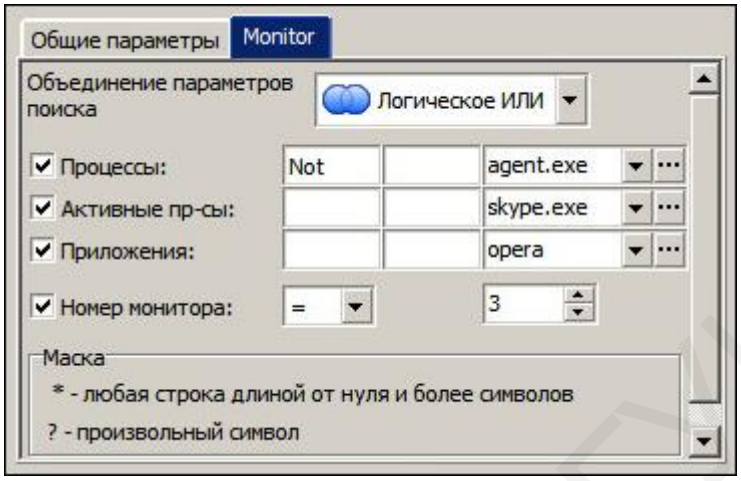


Рис. 3.28. Ограничение поиска снимков экрана

Таблица 3.17

Атрибуты снимков экрана

Атрибут	Назначение
Процессы	Имя процесса, запущенного в операционной системе компьютера на момент снятия скриншота агентом
Активные процессы	Имя процесса, который был активен в момент снятия скриншота агентом
Приложения	Название проиложения, которое было активно в момент снятия скриншота агентом
Номер монитора	Номер монитора, на котором происходило снятие скриншота

Ограничения по атрибутам Lync-сообщений настраиваются на вкладке «Lync» (рис. 3.29). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам. Назначение используемых атрибутов указано в табл. 3.18.

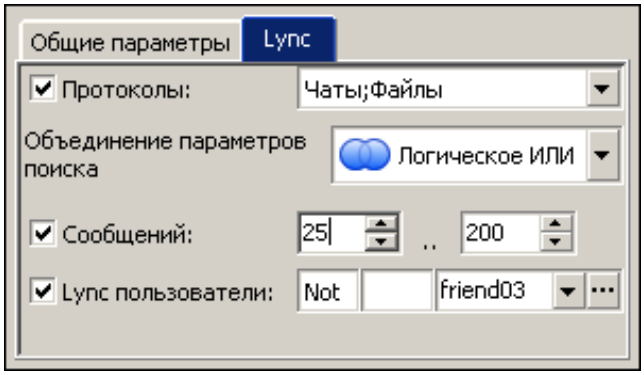


Рис. 3.29. Ограничение по атрибутам Lync-сообщений

Библиотека БГУИР

Таблица 3.18

Атрибуты Lync-сообщений

Атрибут	Назначение
Протоколы	Выбор типа перехваченого документа: чаты, звонки, файлы. Для выбора установите флажок. Если не выбран ни один тип документа, поиск будет произведен с настройками по умолчанию – по всем типам документов
Сообщений	Количество сообщений между пользователями Lync
Lync пользователи	Идентификатор пользователя Lync

Ограничения по атрибутам записей журналов Active Directory настраиваются на вкладке «ADSniffer» (рис. 3.30). Назначение атрибутов указано в табл. 3.19.

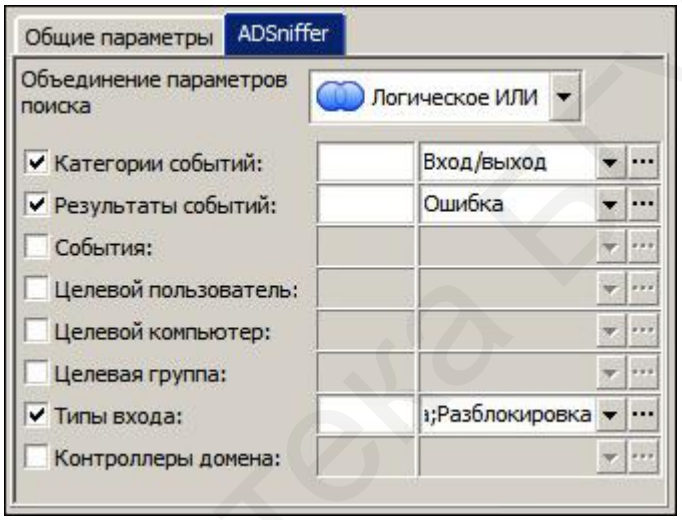


Рис. 3.30. Ограничение по атрибутам ADSniffer

Таблица 3.19

Атрибуты ADSniffer

Атрибут	Назначение
Категория событий	Выбор категорий событий журналов Active Directory: вход/выход, система и др.
Результаты событий	Выбор результатов событий: ошибка, предупреждение, информация, успешно, отказано
События	Выбор событий: вход с учетной записью выполнен успешно, учетной записи не удалось выполнить вход в систему и др.
Целевой пользователь	Выбор пользователей для поиска в записях журналов Active Directory по полю «Целевой пользователь»
Целевой компьютер	Выбор компьютеров для поиска в записях журналов Active Directory по полю «Целевой компьютер»
Целевая группа	Выбор группы для поиска в записях журналов Active Directory по полю «Целевая группа»
Типы входа	Выбор типа входа: не задан, сетевой, служба, разблокировка и др.
Контроллеры домена	Выбор контроллеров домена

Библиотека БГУИР

Ограничения по атрибутам документов рабочих станций корпоративной сети настраиваются на вкладке «Workstation» (рис. 3.31). Основные подходы к настройке ограничений совпадают с теми, которые были описаны применительно к рассмотренным ранее типам подключенных индексов. Назначение используемых атрибутов указано в табл. 3.20.

Таблица 3.20

Атрибуты документов рабочих станций корпоративной сети, по которым возможно ограничение поиска

Атрибут	Назначение
Дата создания	Дата создания индекса, содержащего документы рабочих станций сети
Дата обновления	Дата последнего обновления индекса

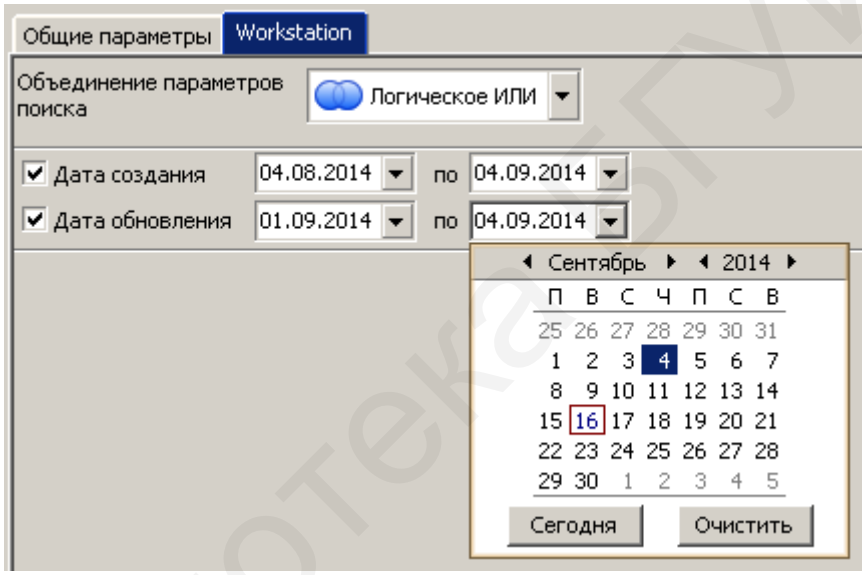


Рис. 3.31. Ограничение поиска по атрибутам документов рабочих станций корпоративной сети

Даты могут указываться как вручную, так и при помощи календаря.

При поиске по индексам Workstation необходимо помнить следующее:

– поиск по доменам не производится (кроме случаев, когда указан домен и установлен флажок в строке «Исключая»);

– поиск документов по доменным пользователям, указанным на вкладке «Общие параметры», невозможен;

– флажок в строке «SSL» на вкладке общих параметров должен быть снят.

Панель результатов включает в себя следующие элементы управления:

– выпадающий список «Фильтр по индексам» позволяет осуществить выбор результатов поиска по отдельному индексу либо по всем индексам в целом (опция «Все результаты»);

– кнопка «Все результаты» отображает полный список результатов вне зависимости от настройки числа отображаемых документов. Полный список результатов будет привязан к позиции, выбранной в выпадающем списке «Фильтр по индексам»;

Библиотека БГУИР

– кнопка «Табличный просмотр / Детальный просмотр» предназначена для выбора режима просмотра результатов поиска;

– кнопка «Экспорт списка» позволяет экспортировать список результатов в файлы форматов XLS, XML, HTML или TXT;

– при помощи кнопки «Поиск похожих» осуществляется поиск документов, похожих по содержанию на выделенный;

– кнопка «Атрибуты (Свойства) документа» открывает окно свойств документа;

– кнопка «Свойства пользователя» открывает окно свойств пользователя;

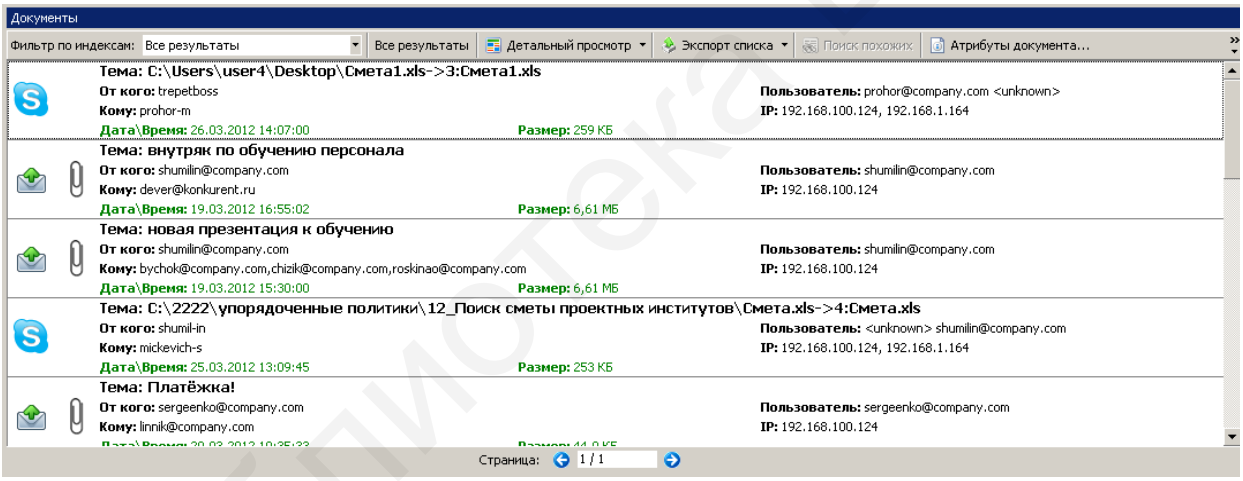
– кнопка «История переписки» отображает все сообщения, входящие в историю переписки двух пользователей.

Для отображения результатов могут использоваться два режима просмотра (рис. 3.32):

– детальный просмотр (данные по свойствам каждого найденного сообщения имеют более компактный вид);

– табличный просмотр (свойства сообщения систематизированы по столбцам).

Детальный просмотр



Табличный просмотр

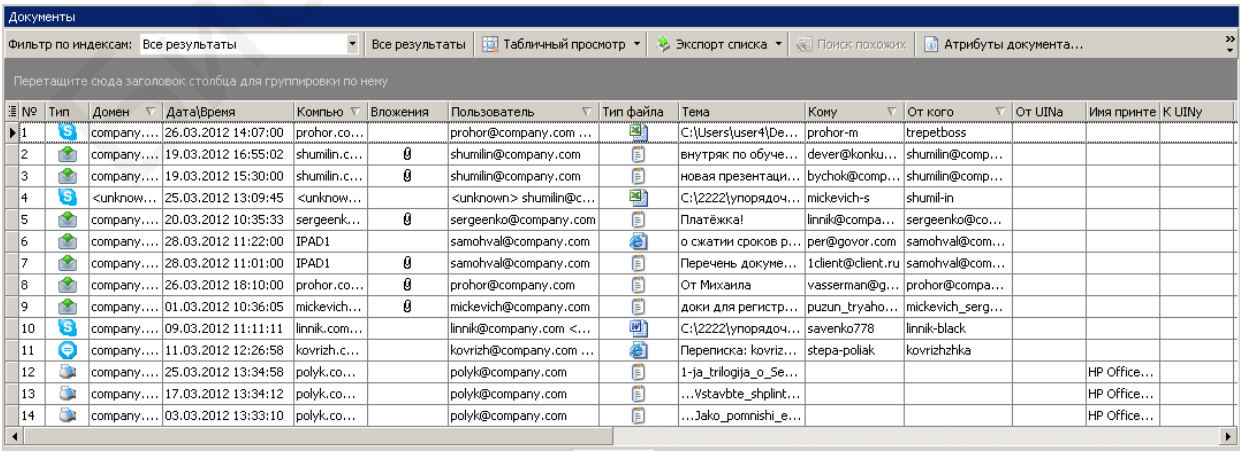


Рис. 3.32. Режимы просмотра панели результатов

Библиотека БГУИР

Документы в результатах выдачи могут маркироваться разными цветами:

– красным – в случае, когда из файла не удалось извлечь текст;

– зеленым – если при передаче данных использовалось безопасное соединение (протокол SSL);

– голубым – при наличии HTTP GET-запросов;

– серым цветом обозначается черновой вариант электронного сообщения, сохраненный в процессе его создания.

На панели результатов в табличном режиме просмотра отображаются следующие столбцы:

– **№** – отображает номер документа по порядку;

– **Тип** – тип канала передачи данных, по которому передавался документ. Отображает также направление движения данных (Mail) или тип сеанса связи (Skype);

– **Вложения** – отметка о наличии в сообщении вложенного файла;

– **Дата\Время** – дата и время перехвата документа;

– **Тип файла** – файловый формат документа (отображается в виде значка формата файла);

– **Тема** – тема электронного сообщения (для Mail); путь к переданному файлу или перечень участников переписки (для Skype); заголовок/имя распечатываемого документа (для Print);

– **От кого** – имя и адрес отправителя;

– **От UINa** – идентификационный номер пользователя, отправившего сообщение;

– **Кому** – имя и адрес адресата;

– **К UINy** – идентификационный номер пользователя, принявшего сообщение;

– **Домен** – наименование домена;

– **Компьютер** – имя компьютера отправителя;

– **Пользователь** – имя учетной записи отправителя;

– **От/к IP** – IP-адрес отправителя/получателя;

– **MAC** – MAC-адрес сетевого адаптера отправителя;

– **Размер** – размер документа;

– **Полное имя** – имя пользователя, полученное из Active Directory (заполняется при включенном режиме интеграции с DataCenter);

– **Участников** – количество участников диалога;

– **Сообщений** – число сообщений в текущем документе;

– **Имя файла** – название файла, передаваемого на внешнее устройство;

– **Тип устройства** – вид подключаемого внешнего устройства;

– **Имя устройства** – назначенное производителем либо пользователем имя устройства;

– **Серийный номер** – уникальный номер устройства, присвоенный производителем при изготовлении;

– **<->** – направление передачи документа по FTP-соединению;

– **FTP сервер** – IP-адрес FTP-сервера;

Библиотека БГУИР

– **FTP логин** – идентификатор, используемый пользователем для подключения к FTP-серверу;

– **Имя принтера** – принтер, на котором был распечатан документ;

– **Страниц** – количество отправленных на принтер страниц;

– **Дата создания** – дата создания электронного сообщения (или индекса);

– **Запрос** – текст HTTP-запроса;

– **Дата обновления** – дата последнего обновления индекса;

– **Старое имя** – предыдущее имя файла до его переименования;

– **Тип устр-ва** – вид устройства хранения документа, с которым совершалась файловая операция;

– **Окончание** – дата и время завершения записи разговора (для Microphone) или логирования нажатия клавиш в запущенном приложении (для KeyLogger);

– **Процесс/Образ** – путь к исполнимому файлу, из которого операция выполнялась;

– **Создание/Чтение/Запись/Удаление/Переименование/Выполнение** – тип произведенной файловой операции;

– **Подключение/Отключение/Открытие/Форматирование** – тип произведенного действия с подключенным внешним устройством;

– **Производитель** – производитель подключаемого внешнего устройства;

– **Действия** – тип операции, произведенной с файлом (для DeviceSniffer);

– **Длительность** – продолжительность звукового файла (для Microphone) или времени, проведенного в приложении (для KeyLogger и ProgramSniffer);

– **Логин/Пароль** – данные, вводимые пользователем при авторизации на веб-сервере;

– **Микрофон** – название используемого для звукозаписи микрофона в системе;

– **Категория** – краткое имя продукта;

– **ID** – уникальный идентификационный номер документа;

– **SID пользователя** – идентификатор безопасности;

– **Номер монитора** – номер монитора, на котором происходило снятие скриншота;

– **Результат** – результат события в журнале безопасности Active Directory;

– **Категория события** – категория события в журнале безопасности Active Directory;

– **Сетевой интерфейс** – сетевая карта, на которой были перехвачены данные;

– **Событие** – событие в журнале безопасности Active Directory;

– **Целевой пользователь** – запись в поле «Целевой пользователь» журналов безопасности Active Directory;

– **Целевой компьютер** – запись в поле «Целевой компьютер» журналов безопасности Active Directory;

Библиотека БГУИР

– **Целевая группа** – запись в поле «Целевая группа» журналов безопасности Active Directory;

– **Метки** – флажок «Обратить внимание»;

– **IP-адрес** – IP-адрес компьютера (для ADSniffer);

– **Контроллер домена** – имя контроллера домена;

– **Релевантность** – процент схожести документа с образцом;

– **Документ образец** – документ, с которым будет сравниваться каждый документ в подключенном индексе и/или базе данных на предмет схожести;

– **Текст** – часть текста (первые 100 симоволов), вводимая пользователем с клавиатуры (KeyloggerSniffer).

Щелчком кнопки мыши по заголовку столбца результаты поиска сортируются в прямом либо обратном порядке по данному параметру.

В левом верхнем углу таблицы расположена кнопка-значок  , позволяющая настроить отображение столбцов. С помощью установки/снятия флажков в выпадающем списке заголовков столбцов можно отобразить/скрыть те или иные столбцы. Перемещение столбцов осуществляется обычным перетаскиванием при помощи кнопки мыши.

Очередность следования столбцов можно также менять перетаскиванием ячеек с названием столбца в самой таблице.

Результаты поиска можно группировать по заголовкам столбцов. Для этого с помощью кнопки мыши нужно перетащить одну или несколько ячеек с заголовком столбца в область с надписью «Перетащите сюда заголовок столбца для группировки по нему». В таблице сгруппированные результаты будут отображены с соблюдением указанной иерархии (рис. 3.33).

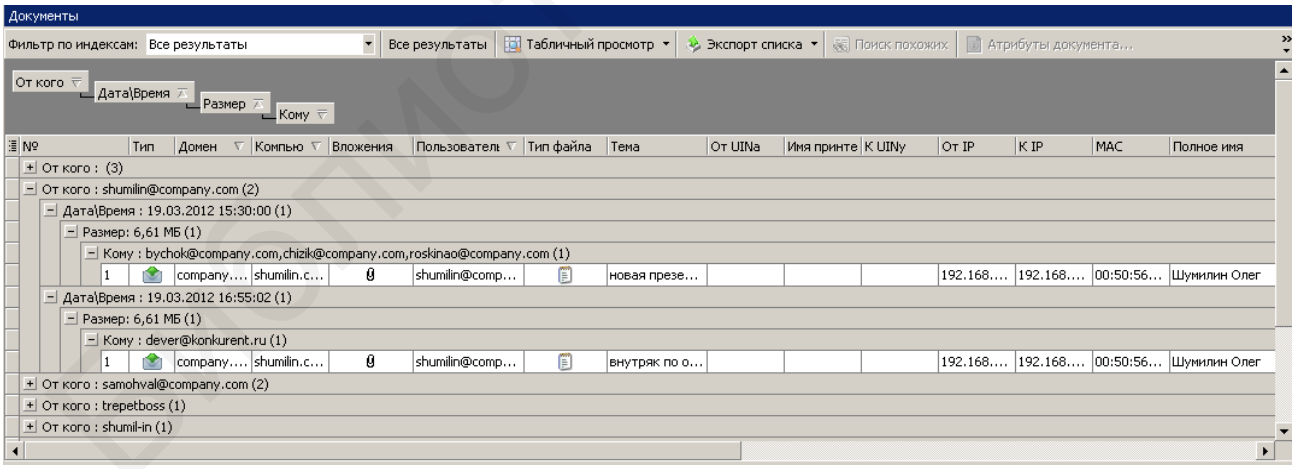


Рис. 3.33. Группировка результатов поиска по заголовкам столбцов

В детальном и табличном режимах просмотра щелчком правой кнопки мыши по документу вызывается контекстное меню, содержащее следующие команды:

– «Открыть документ» – открывает выделенный документ в отдельном окне;

– «Сохранить документ как...» – сохраняет выделенный документ в виде файла;

– «Поиск похожих» – поиск документов, похожих по содержанию на выделенный;

– «История переписки» – отображает все сообщения, входящие в историю переписки двух пользователей;

– «Атрибуты документа» – открывает окно свойств документа;

– «Восстановить настройки таблицы» – сбрасывает все настройки (скрытие, порядок расположения, группировка), произведенные пользователем над столбцами результатов поиска. При этом скрытые по умолчанию колонки остаются скрытыми.

При выделении документа его содержимое отображается в окне предпросмотра, расположенном в правом нижнем углу главного окна клиента (рис. 3.34).

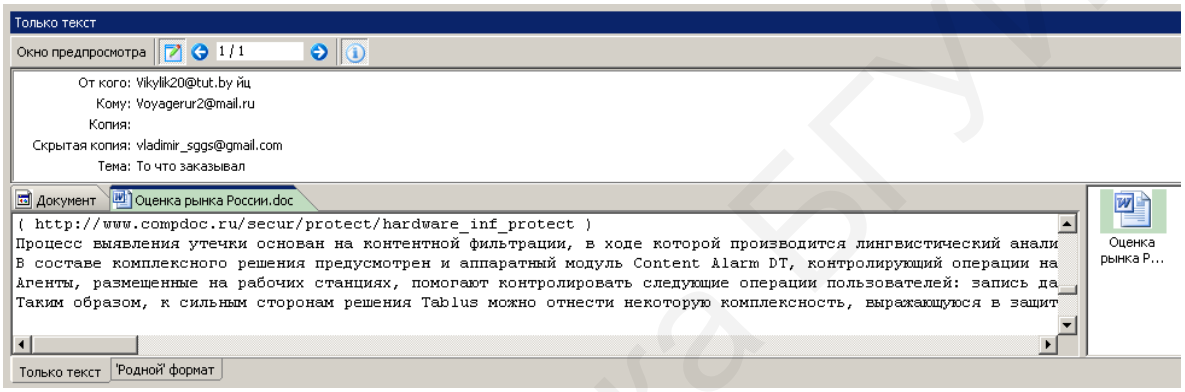


Рис. 3.34. Окно предпросмотра

В верхней части окна предпросмотра расположены следующие элементы управления:

– кнопка – для включения/отключения подсветки слов запроса (цвет подсветки можно изменить в настройках клиента);

– кнопки и – для перехода к предыдущему/следующему подсвеченному слову;

– кнопка – для отображения/скрытия дополнительной информации по документу.

В нижней части окна настраивается режим отображения окна предпросмотра: «Только текст» или «'Родной' формат». В режиме «Только текст» содержимое документа будет отображаться как простой текст. В режиме «'Родной' формат» будут сохраняться элементы формата исходного письма (таблицы, фон, шрифт, выделение и т. п.).

Если в результате проведения поискового запроса совпадения были найдены внутри прикрепленного файла, то при условии включения подсветки найденных слов он будет взят в цветную рамку для акцентирования внимания. В режиме просмотра «Только текст» будет отображена дополнительная вкладка для просмотра и перемещения по подсвеченным словам вложенного файла.

Библиотека БГУИР

Настройка псевдонимов. По умолчанию при поиске по индексу IMSniffer на панели результатов отображаются идентификационные номера (UIN) пользователей. Если оригинальные псевдонимы ICQ не дают достаточной информации о личности пользователя, их можно изменить, выполнив последовательность действий:

1. В меню «Файл» выбрать пункт «Настройки псевдонимов».

2. Для добавления псевдонима в появившемся окне воспользоваться кнопкой «Добавить псевдоним», после чего в соответствующие поля ввести значение UIN и его псевдоним (рис. 3.35).

3. Управление имеющимся списком псевдонимов производится с помощью следующих кнопок:

– «Добавить псевдоним» – добавление нового псевдонима для UIN;

– «Редактировать» – корректировка данных выделенного псевдонима;

– «Удалить» – удаление выделенного псевдонима;

– «Экспорт» – сохранение списка псевдонимов во внешний *.txt-файл;

– «Импорт» – импортирование *.txt-списка псевдонимов;

– «Закрыть» – выход из окна «Настройка псевдонимов».

4. В случае когда список достигает больших размеров, можно воспользоваться поиском/фильтрацией по UIN либо псевдониму.

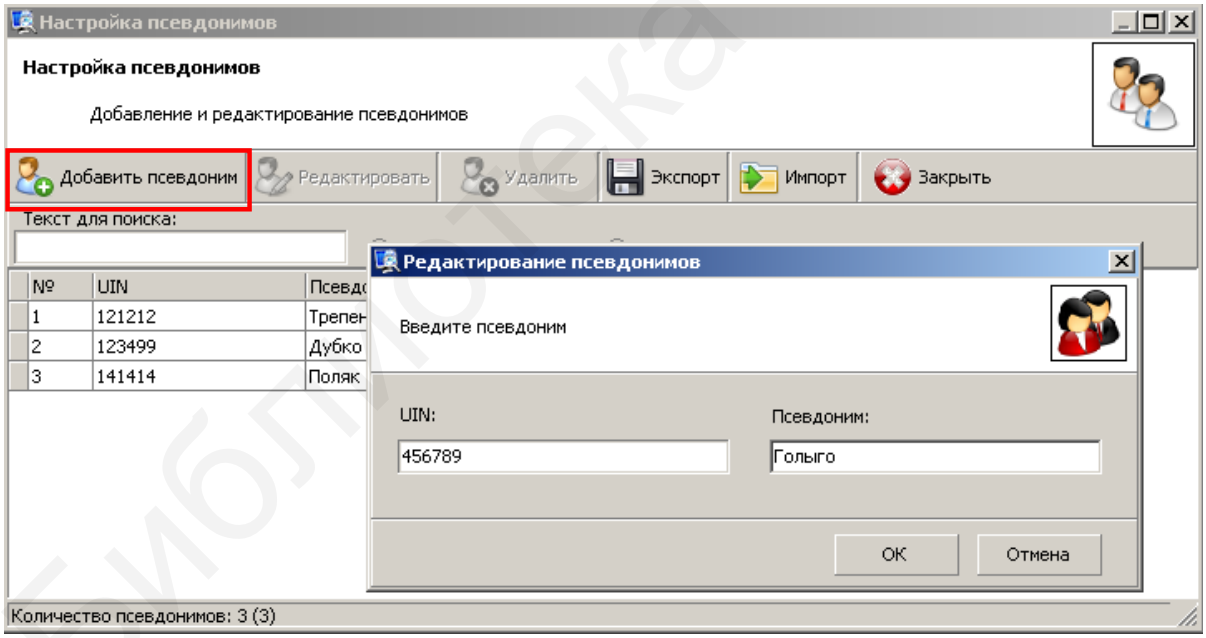
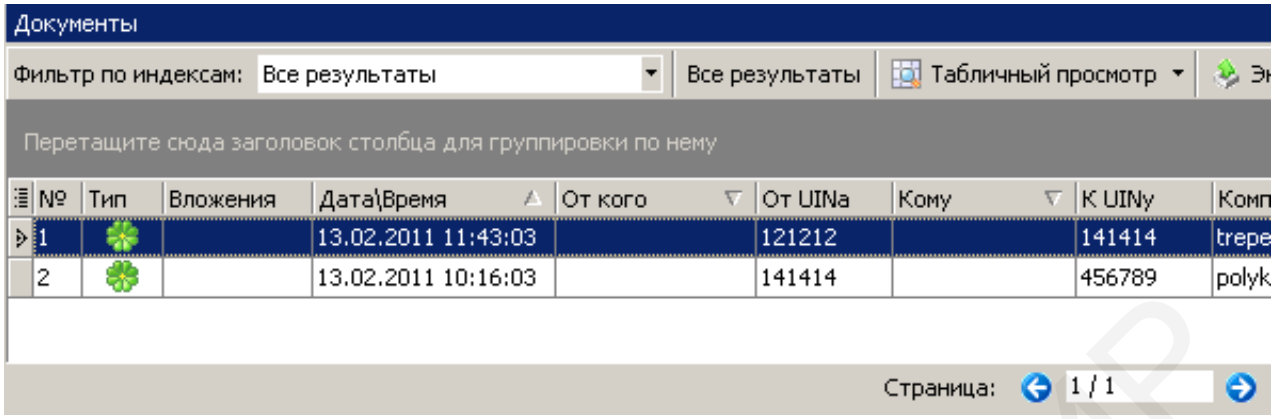


Рис. 3.35. Добавление псевдонима

В результате произведенной настройки в списке документов отображаются новые псевдонимы (рис. 3.36).

Библиотека БГУИР

До редактирования псевдонимов



После редактирования псевдонимов

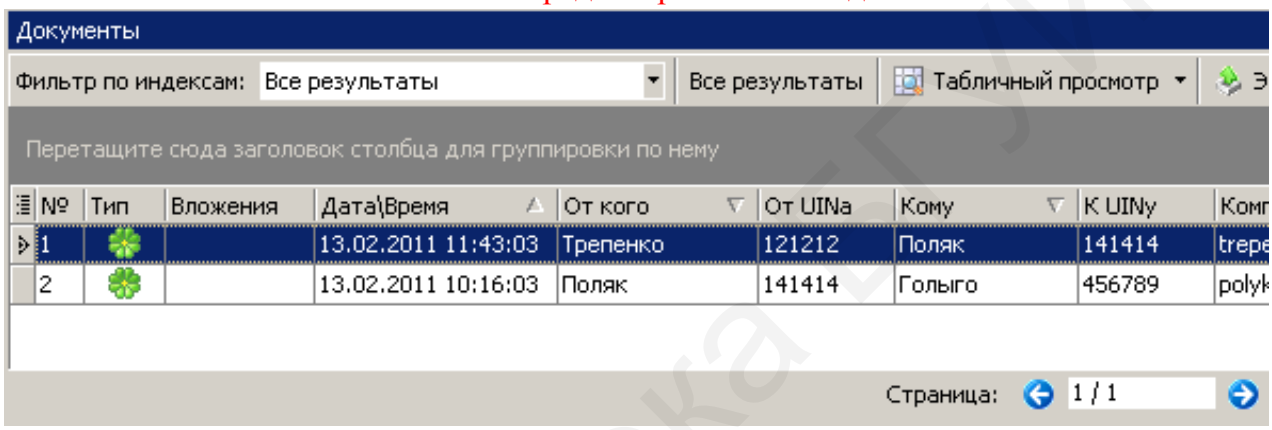


Рис. 3.36. Отображение в списке документов новых псевдонимов

Видеоплеер. Встроенный видеоплеер позволяет просматривать записи действий на экранах сотрудников, а также соотносить видеозаписи с активностью приложений и нажатиями клавиш.

Переход к окну «Просмотр снимков экрана» осуществляется двойным щелчком кнопки мыши по эскизу видеозаписи (рис. 3.37).

В нижней части окна «Просмотр снимков экрана» расположены параметры просмотра (рис. 3.38):

1 – полоса прокрутки видеозаписей. Красный цвет означает, что запись в этот промежуток времени не велась.

2 – кнопки управления воспроизведением, скоростью воспроизведения, переключением между экранами, параметрами размеров окна, датой видеозаписей.

3 – кнопки настроек экспорта, сохранения кадра и видеозаписи (в формате .vid), поиска по данным ProgramSniffer и Keylogger, перехода к режиму LIveView.

Примечание. Для просмотра видеозаписи используется Windows Media Player/Media Player Classic (×32/×64) с установленным видеокодеком SearchInform.

Библиотека БГУИР

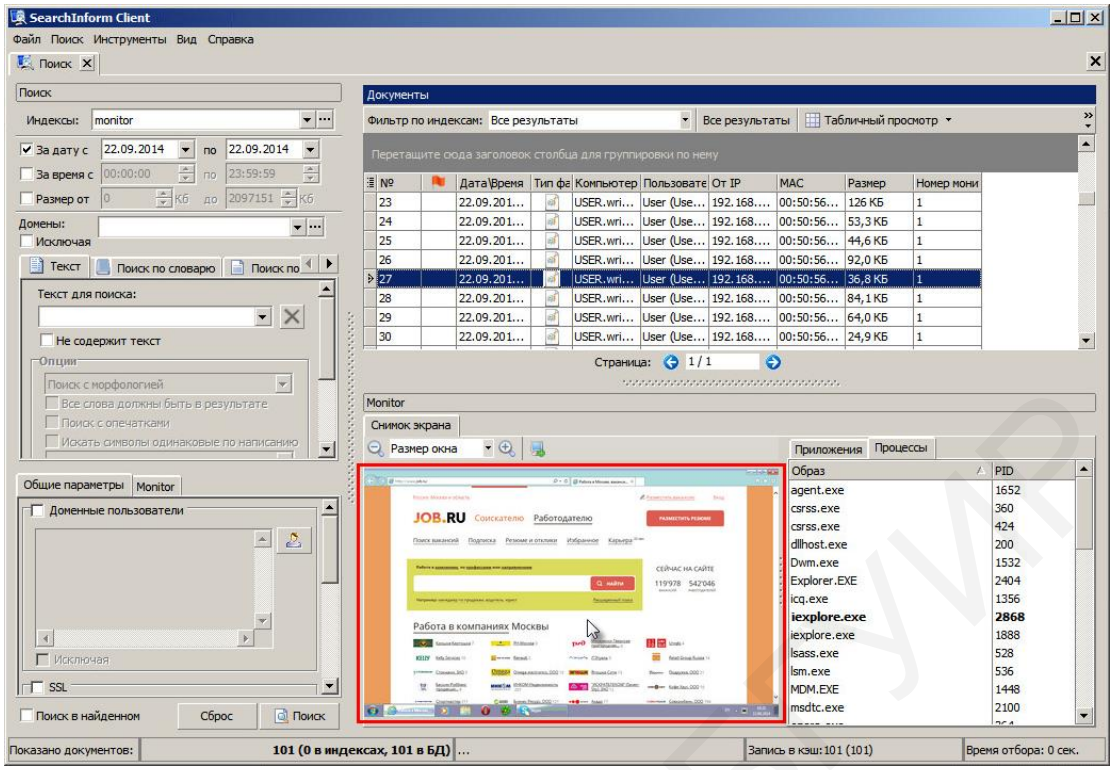


Рис. 3.37. Переход в режим просмотра

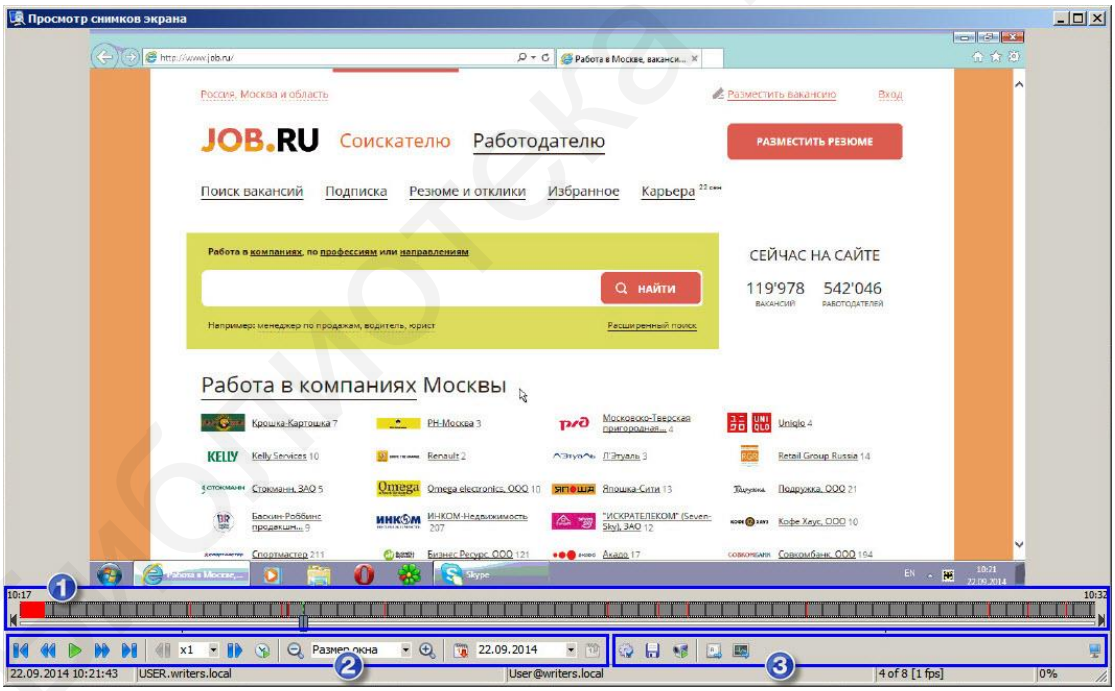


Рис. 3.38. Окно видеоплеера

Для соотнесения активности в приложениях с записанным видео используйте кнопку «ProgramSniffer». В открывшемся окне выберите базу данных ProgramSniffer, в поле поиска введите интересующее приложение/сайт. В поле «Результаты» выберите приложение/сайт и укажите временной промежуток его активности. Будет открыта видеозапись, соответствующая заданному временному промежутку активности (рис. 3.39).

Библиотека БГУИР

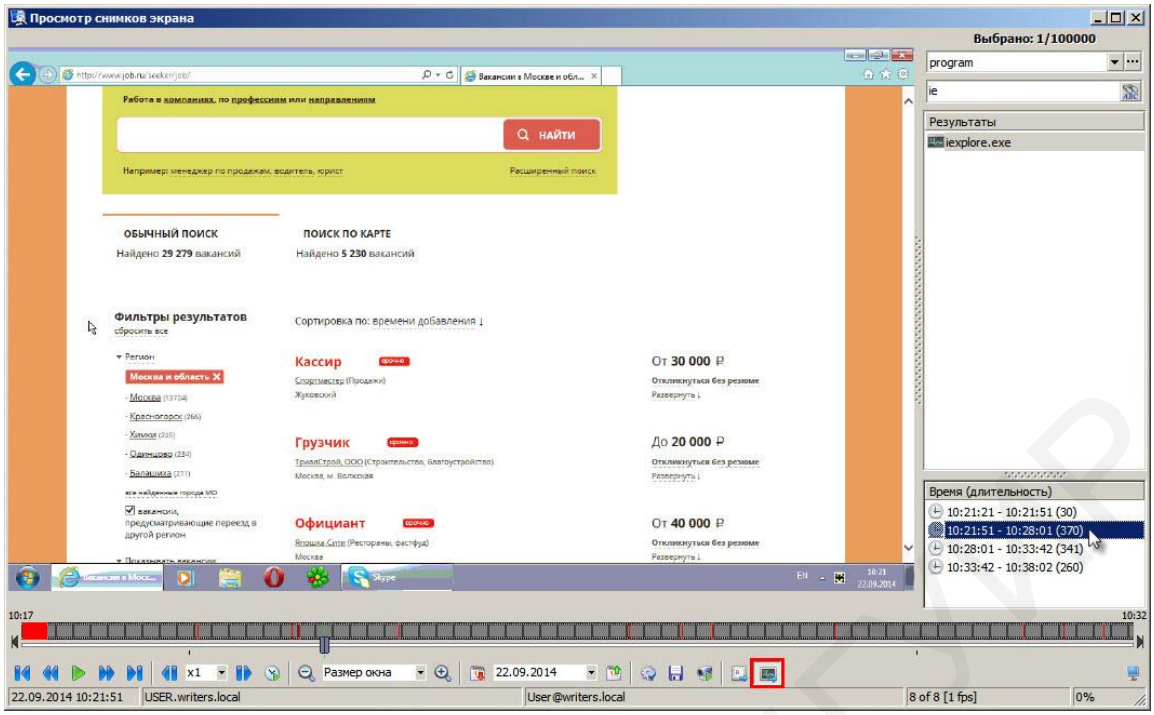


Рис. 3.39. Соотнесение активности процессов и видео

Аналогичным образом можно соотнести с записанным видео и информацию из БД Keylogger (используется кнопка «Keylogger») (рис. 3.40).

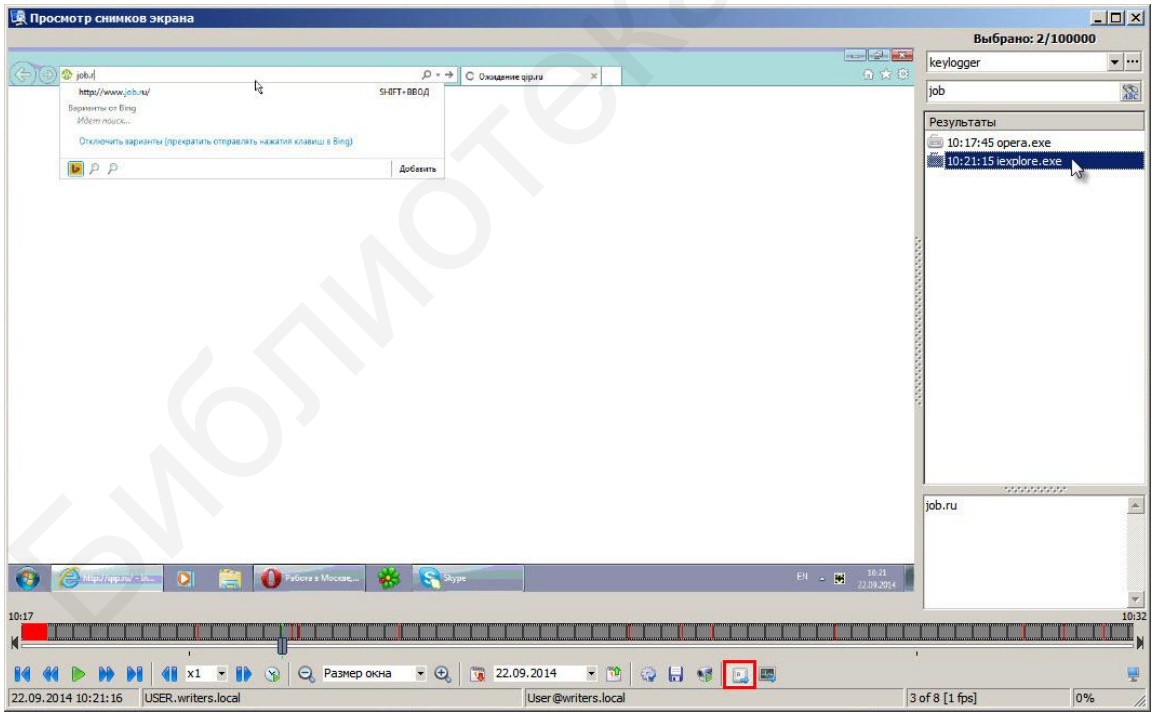


Рис. 3.40. Соотнесение перехвата нажатий клавиш и видео

Библиотека БГУИР

3.2. Автоматический мониторинг информационных потоков при помощи приложения SearchInform AlertCenter

Общая характеристика приложения SearchInform AlertCenter. Приложение SearchInform AlertCenter предназначено для автоматического мониторинга информационных потоков с возможностью уведомления сотрудника службы безопасности о случаях нарушения политик информационной безопасности в отношении передаваемых данных.

AlertCenter имеет клиент-серверную архитектуру, обычно устанавливается на выделенный сервер, обеспечивая проверку перехваченных документов и отправку уведомлений в случае совпадений по введенным запросам. Клиентская часть, как правило, устанавливается на рабочую станцию сотрудника службы безопасности для настройки политик проверки перехваченных документов.

Сервер AlertCenter поддерживает индексы, созданные компонентами DLP-системы «Контур информационной безопасности SearchInform». Благодаря поддержке и взаимодействию всех приложений КИБ AlertCenter обеспечивает мониторинг:

– документов, хранящихся на жестких дисках рабочих станций домена;

– данных, передаваемых на внешние устройства, такие как USB-Flash-накопители, CD/DVD-диски, внешние винчестеры, Bluetooth-адаптеры и т. д.;

– входящего и исходящего трафика по FTP-соединению;

– сообщений, отправленных в форумы, блоги и иные сервисы при помощи веб-форм, поддерживающих GET- и POST-методы;

– сообщений IM-клиентов (ICQ, MSN, QIP и др.), а также сообщений в социальных сетях (Facebook, LinkedIn, В Контакте и др.);

– сообщений электронной почты, отправленных при помощи клиентов или с почтовых веб-сервисов;

– историй операций с файлами, расположенными на файл-серверах или рабочих станциях;

– речи сотрудников;

– содержимого мониторов рабочих станций пользователей;

– документов, распечатанных на локальных и сетевых принтерах;

– сеансов текстовой и голосовой связи, файлов и SMS-сообщений, отправленных через Skype;

– сеансов текстовой и голосовой связи, а также файлов, отправленных через Microsoft Lync;

– сеансов текстовой и голосовой связи, списка контактов и файлов, отправленных через Viber.

Принцип работы SearchInform AlertCenter (рис. 3.41). Приложение по заданному расписанию или по команде пользователя производит поиск по индексам, сформированным в результате перехвата электронной почты, протокола передачи файлов, IM-клиентов, принтера, скайпа и других каналов коммуникации.

Библиотека БГУИР

Индексы формируются сервером индексации SoftInform Search Server, от которого AlertCenter получает список ссылок на имеющиеся индексы.

В клиентском модуле AlertCenter создаются и настраиваются политики безопасности, применяемые к перехваченной информации, а также (при необходимости) политики карантина, применяемые к исходящей почтовой корреспонденции. В консоли клиента AlertCenter также могут быть настроены списки исключений пользователей, библиотеки регулярных выражений и цифровых отпечатков.

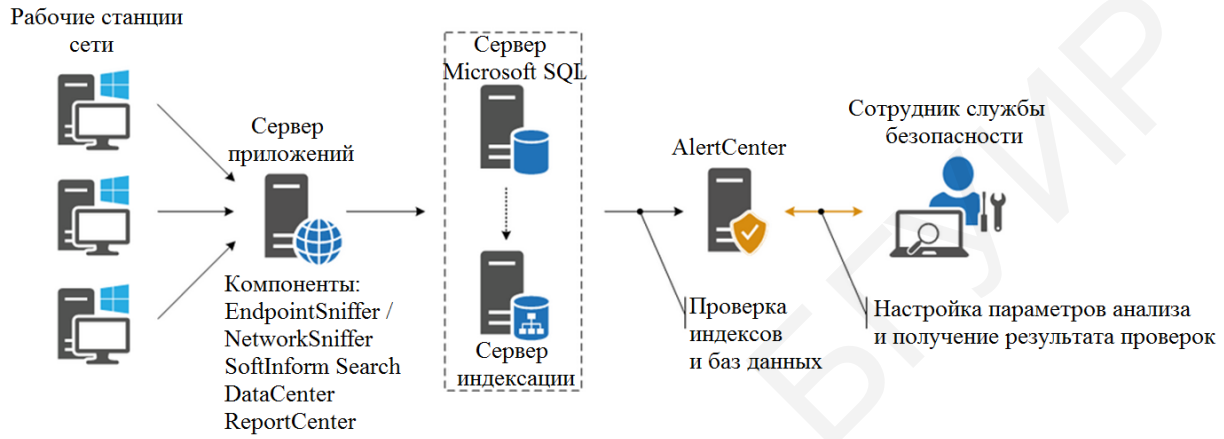


Рис. 3.41. Принцип работы SearchInform AlertCenter

В случае нарушения настроенных в AlertCenter политик безопасности, например, при обнаружении несанкционированной передачи конфиденциальных документов за пределы компании, происходит оповещение сотрудника службы безопасности, на рабочей станции которого находится клиентская часть AlertCenter. Сотрудник службы безопасности производит расследование инцидента с использованием поисковых клиентов КИБ.

На основании настроенных политик карантина подозрительные сообщения электронной почты попадают в карантин, содержимое которого отображается в клиентской части AlertCenter. Решение по отправке задержанных сообщений адресату принимается сотрудником службы безопасности.

Ключевыми функциями/возможностями AlertCenter являются:

– использование двух пользовательских приложений – консоли сервера и клиента AlertCenter;

– хранение всех настроек в базе данных под управлением Microsoft SQL Server;

– гибкая настройка условий проверок при помощи раздельных политик проверки;

– использование поиска по словарю;

– использование поиска по атрибутам и поиска нераспознанных;

– комбинирование простых текстовых и атрибутных запросов при помощи сложных запросов;

Библиотека БГУИР

– использование регулярных выражений;
– использование цифровых отпечатков;
– использование меток;
– использование списка исключений пользователей;
– настройка политик для помещения сообщения в карантин;
– работа с перемещенными в карантин сообщениями;
– настройка блокировки почты;
– ведение журнала событий и журнала результатов;
– открытие документов, по которым зафиксированы инциденты, в клиентах приложений DLP-системы «Контур информационной безопасности SearchInform» и в сопоставленных приложениях;
– настройка словаря синонимов.

Основные характеристики SearchInform AlertCenter представлены в табл. 3.21.

Таблица 3.21

Основные характеристики SearchInform AlertCenter

Характеристика	**Значение**
1	**2**
Технология поиска	SoftInform Search Technology
Типы запросов	▪ Фразовый поиск (поиск по ключевым словам и фразам в тексте). ▪ Поиск по словарю. ▪ Поиск похожих (поиск с использованием целого текста в качестве запроса и с настройкой требуемого показателя совпадения). ▪ Поиск по атрибутам документов. ▪ Поиск нераспознанных документов. ▪ Сложный запрос (поиск по нескольким условиям). ▪ Поиск по регулярным выражениям. ▪ Поиск по цифровым отпечаткам. ▪ Поиск по базам данных
Поддерживаемые индексы	▪ Device. ▪ FTP. ▪ HTTP. ▪ IM. ▪ Lync. ▪ Mail. ▪ Print. ▪ Skype. ▪ Viber. ▪ SoftInform Search Server (в том числе функции, включенные в состав сервера индексации рабочих станций)
Число подключаемых индексов	Не ограничено
Уведомления	▪ Отправка в сообщениях электронной почты по протоколу SMTP. ▪ Отправка в архиве, защищенном паролем

Библиотека БГУИР

Окончание табл. 3.21

1	2
Поддерживаемые компоненты КИБ	**Сервер EndpointSniffer** – перехват данных с помощью агентов, установленных на рабочих станциях. На платформе EndpointSniffer работают модули перехвата: – CloudSniffer; – DeviceSniffer; – FileSniffer; – FTPSniffer; – HTTPSniffer; – IMSniffer; – LyncSniffer; – MailSniffer; – MicrophoneSniffer; – MonitorSniffer; – PrintSniffer; – SkypeSniffer; – ViberSniffer. **Сервер NetworkSniffer** – перехват трафика на уровне сетевых шлюзов. Включает следующие модули перехвата: – CloudSniffer; – FTPSniffer; – HTTPSniffer; – IMSniffer; – MailSniffer; – ADSniffer. **SearchInform Client** – поиск в сообщениях, переданных по различным каналам коммуникации (веб-формы, мессенджеры, скайп, электронная почта и т.д.). **SearchInform DataCenter** – управление всеми индексами и базами данных, которые были созданы компонентами программного комплекса. **SearchInform ReportCenter** – сбор статистики и генерация отчетов по активности пользователей и фактам нарушения политик информационной безопасности. **SoftInform Search Server** – поиск в файлах, расположенных на жестких дисках рабочих станций сети

Состав AlertCenter. Рассматриваемый компонент включает в себя две части, взаимодействующие друг с другом посредством обращений к общей базе данных под управлением Microsoft SQL Server версии 2005 и выше, – серверную и клиентскую:

– серверный модуль читает информационные потоки, проверяет документы, идентифицирует конфиденциальные документы и оповещает администратора безопасности в случае наличия инцидентов;

– клиентский модуль обеспечивает настройку правил проверки (в соответствии с которыми идентифицируются конфиденциальные документы) и просмотр журнала инцидентов.

Библиотека БГУИР

Функции и интерфейс серверного модуля AlertCenter. Консоль сервера AlertCenter выполняет следующие функции:

– создание новой или выбор существующей базы AlertCenter;
– запуск и остановка сервера AlertCenter;
– настройка уровня логирования работы сервера;
– настройка приоритета выполнения задач;
– настройка количества одновременно выполняемых задач;
– настройка синхронизации с LDAP-каталогом Active Directory;
– настройка службы остановки почты;
– управление лицензиями на пользование продуктом AlertCenter.

В консоли серверной части AlertCenter имеется четыре вкладки (рис. 3.42):

– «База данных» – обеспечивает подключение к базе настроек сервера AlertCenter;

– «Сервер AlertCenter» – обеспечивает запуск и остановку сервера, настройку параметров службы AlertCenter (уровня логирования, приоритета выполнения задач, количества задач, выполняемых одновременно, и параметров синхронизации с Active Directory);

– «Служба остановки почты» – обеспечивает запуск и остановку службы, а также настройку уровня логирования ее работы;

– «Лицензии» – обеспечивает управление лицензиями на пользование продуктом AlertCenter.

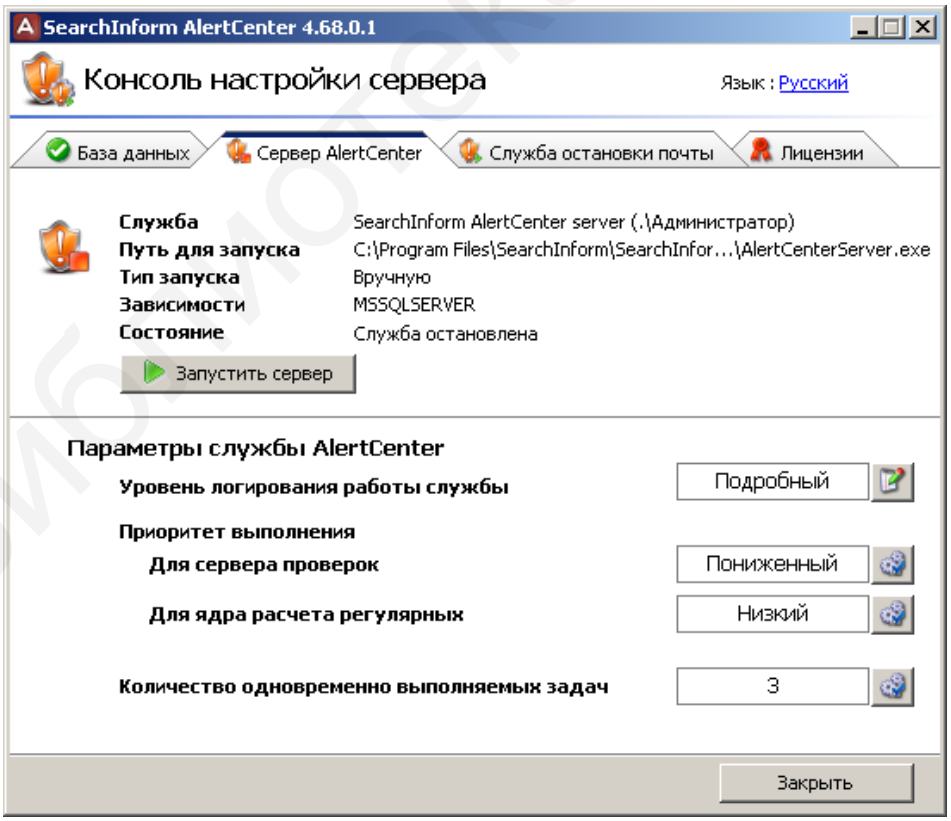


Рис. 3.42. Интерфейс серверного модуля AlertCenter

Библиотека БГУИР

Функции и интерфейс клиентского модуля AlertCenter (рис. 3.43). Клиент AlertCenter предназначен для настройки баз AlertCenter и выполняет следующие функции:

– подключение индексов;

– регистрация пользователей;

– настройка отправки уведомлений;

– настройка списка исключений;

– настройка политик безопасности;

– настройка политик карантина;

– управление журналом инцидентов (просмотр, экспорт, фильтрация);

– управление журналом событий (изменения, сообщения, активные события);

– настройка библиотеки регулярных выражений (включая их экспорт и импорт);

– настройка почты с остановкой;

– управление словарем синонимов.

Рис. 3.43. Интерфейс клиентского модуля AlertCenter

Подключение индексов и баз данных. AlertCenter получает информацию об индексах, связях (серверы, продукты, цепочки), базах данных от продукта DataCenter и кэширует ее в базе данных AlertCenter. Смонтированными считаются все индексы и базы данных, которые известны продукту DataCenter и имеют статус доступных для поиска.

Для просмотра всех доступных для поиска индексов и баз данных следует перейти в узел настроек «Смонтированные индексы» (рис. 3.44).

Библиотека БГУИР

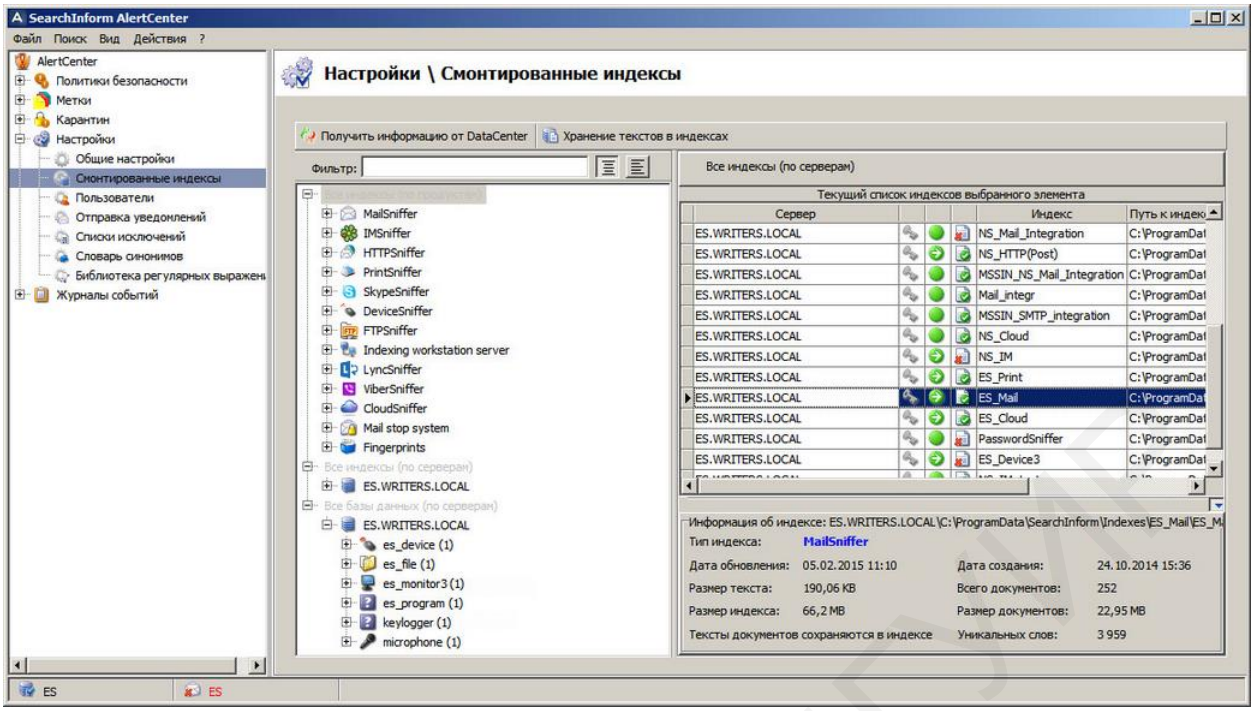


Рис. 3.44. Смонтированные индексы

Далее необходимо нажать кнопку «Получить информацию от DataCenter». По умолчанию подключение производится к серверу DataCenter, указанному при установке DataCenter API или агента DataCenter. В общем случае для задания сервера DataCenter следует выбрать команду «Администрирование» в меню «Файл» и перейти на вкладку «Сервер DataCenter». Для указания сервера DataCenter, к которому будет происходить подключение посредством DataCenter API, можно воспользоваться кнопкой «Изменить».

Смонтированные индексы могут быть сгруппированы по продуктам либо по серверам SoftInform Search.

В группе «Все индексы (по продуктам)» содержатся цепочки и индексы сервера SoftInform Search, определенного продуктом DataCenter по умолчанию.

Группа «Все индексы (по серверам)» содержит список серверов SoftInform Search. При раскрытии сервера можно увидеть цепочки и список составляющих эти цепочки индексов, привязанных к данному серверу индексации.

Базы данных группируются по серверам SoftInform Search.

В группе «Все базы данных (по серверам)» содержится список серверов SoftInform Search. При раскрытии сервера можно увидеть список баз данных, привязанных к данному серверу индексации.

В случаях когда на сервере индексации SoftInform Search Server выставлены дополнительные параметры авторизации, для доступа к индексу следует нажать кнопку «Параметры авторизации» либо выбрать команду «Параметры доступа к серверу» из контекстного меню (рис. 3.45).

Библиотека БГУИР

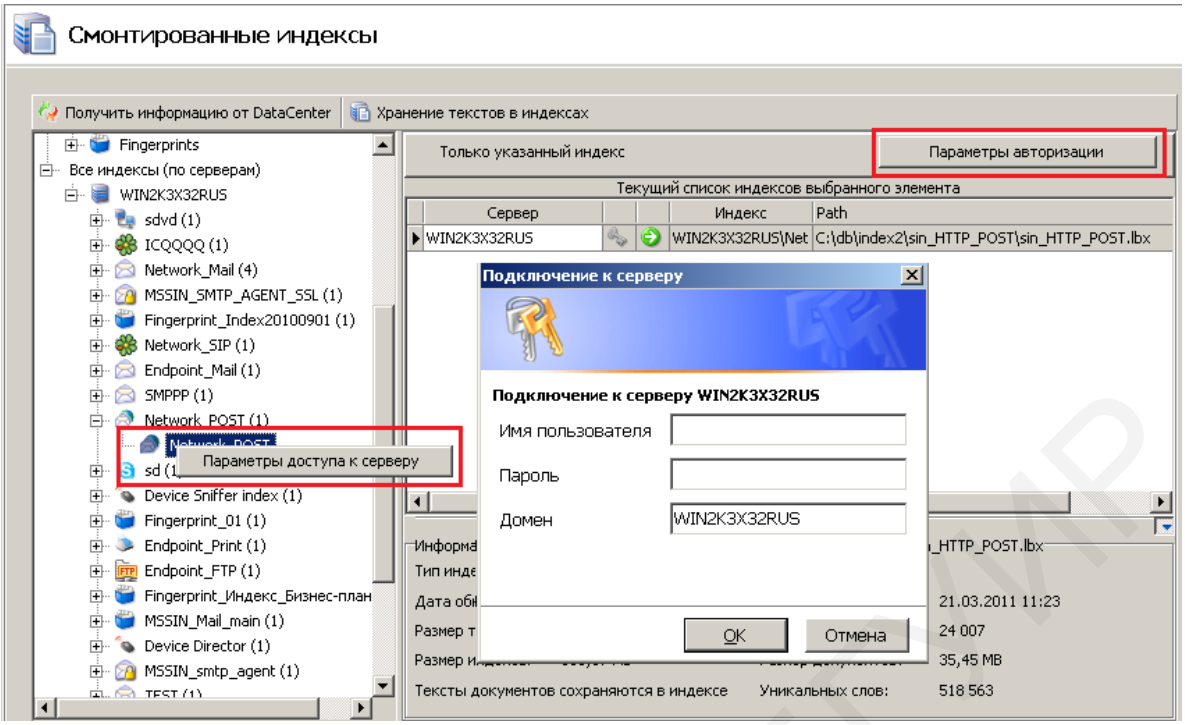


Рис. 3.45. Авторизация с целью получения доступа к индексу

В окне авторизации необходимо ввести имя пользователя, домен и пароль для подключения к серверу, после чего нажать кнопку «ОК». Чтобы избежать ввода параметров авторизации каждый раз для доступа к отдельному индексу, достаточно один раз авторизоваться относительно самого сервера индексации (рис. 3.46).

Индексы, подключенные с помощью дополнительных параметров авторизации, обозначаются в списке значком в виде желтого ключа (рис. 3.47).

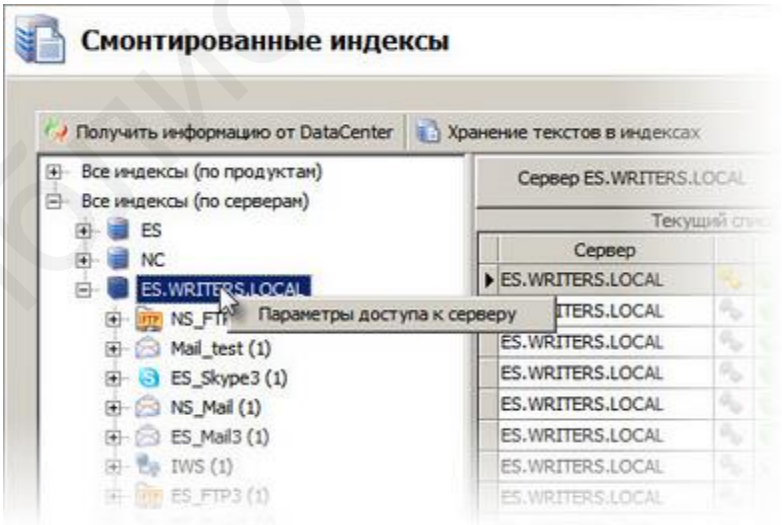


Рис. 3.46. Авторизация на сервере индексации

Рис. 3.47. Индекс, подключенный с помощью дополнительных параметров авторизации

Библиотека БГУИР

Регистрация пользователей. Настройка общего списка пользователей производится при помощи клиентского модуля AlertCenter. В общем списке базы настроек должны быть зарегистрированы:

а) пользователи, от имени которых осуществляется доступ к серверу баз данных под управлением Microsoft SQL Server;

б) получатели уведомлений AlertCenter.

Данные пользователей можно вводить вручную или получать из DataCenter/Active Directory. Список пользователей из Active Directory может поступать в AlertCenter либо напрямую, либо с сервера DataCenter. Указанные действия производятся в узле «Настройки» на вкладке «Пользователи» (рис. 3.48). Для добавления пользователя вручную используется кнопка «Новый пользователь», для получения списка пользователей домена из Active Directory – кнопка «Добавить пользователей».

Как уже было отмечено, для добавления пользователя вручную следует нажать кнопку «Новый пользователь». Для каждого пользователя можно задать следующие группы параметров:

– «Общие»;

– «Политики безопасности»;

– «Метки»;

– «Списки исключений».

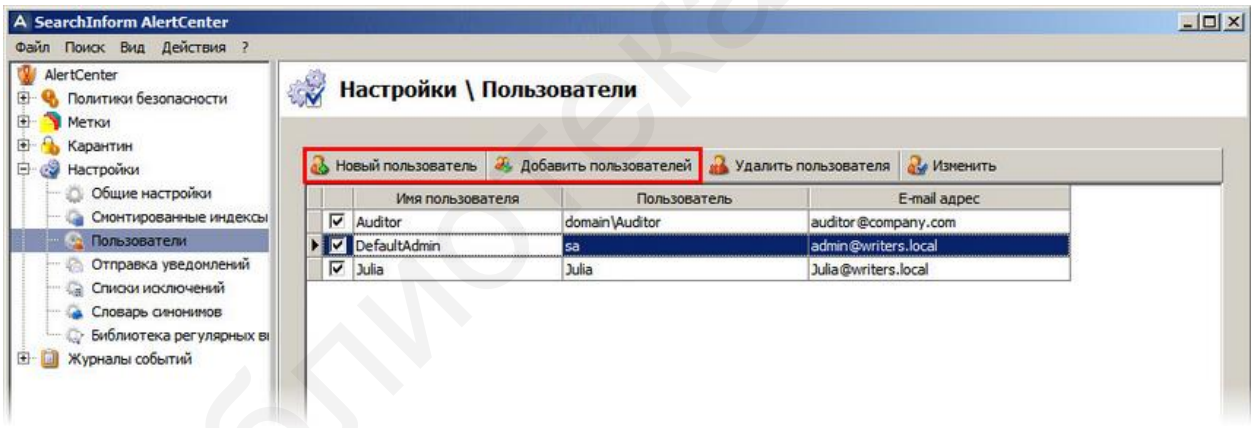


Рис. 3.48. Вкладка «Пользователи»

На вкладке «Общие» (рис. 3.49) необходимо ввести: имя пользователя, доменное имя (можно получить из DataCenter/Active Directory), адрес электронной почты, а также отметить флажком необходимые пункты в перечне «Прочие параметры». К ним относятся:

– «Активен»;

– «Администратор по умолчанию» (строка активна только для системной учетной записи);

– «Администрирование разрешено»;

– «Редактирование параметров разрешено»;

– «Только просмотр».

Библиотека БГУИР

Следует помнить, что только при условии установки флажка в строке «Администрирование разрешено» пользователь может редактировать права других пользователей.

Для выбора доменных пользователей служит кнопка «Добавить пользователей» (см. рис. 3.48). При этом в соответствующем окне необходимо отметить требуемых пользователей и подтвердить выбор кнопкой «Добавить».

На вкладке «Политики безопасности» для каждой из политик индивидуально можно задать права доступа (рис. 3.50):

– «Запрещено» – пользователю недоступны как сама политика, так и результаты проверки по ней;

– «Только просмотр» – пользователь имеет доступ к политике, но без права ее изменения;

– «Изменить» – доступ с правом редактирования.

На вкладке «Метки» задаются права доступа к инцидентам с метками (рис. 3.51). Только при условии установки флажка в строке «Администрирование разрешено» пользователь может редактировать права доступа к меткам.

На вкладке «Списки исключений» задаются права доступа к «белым» и «черным» спискам (рис. 3.52).

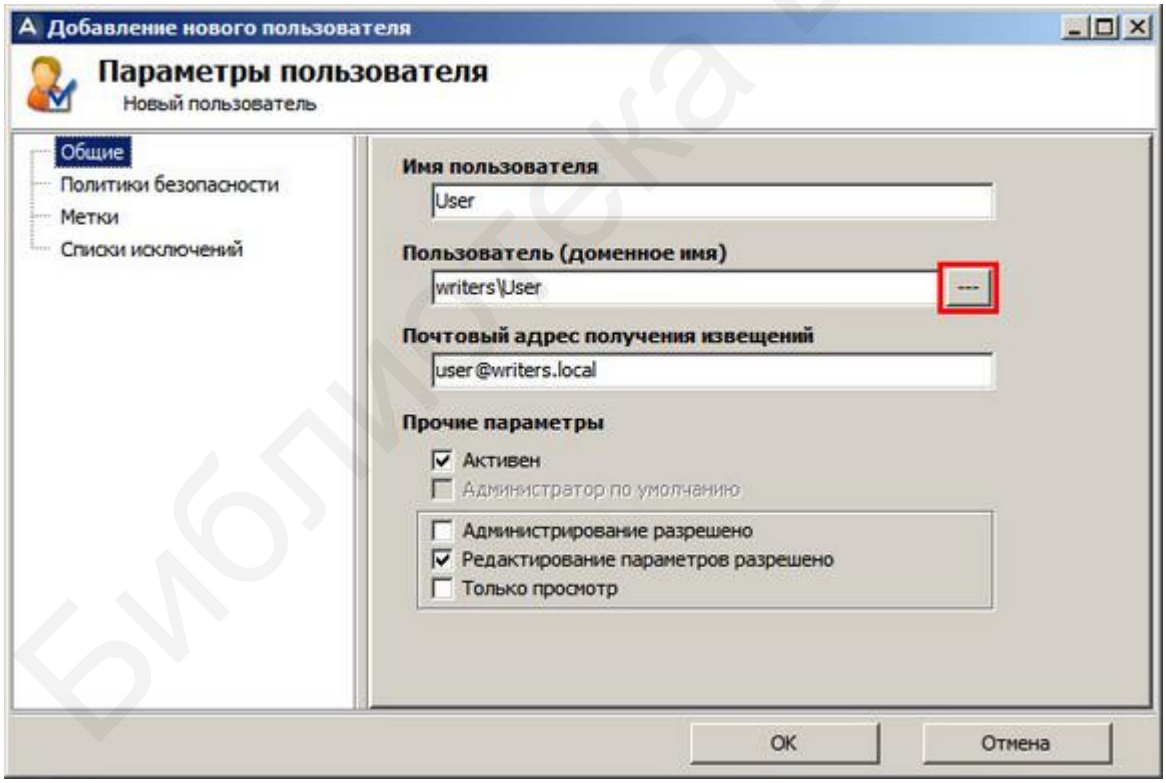


Рис. 3.49. Вкладка «Общие»

Библиотека БГУИР

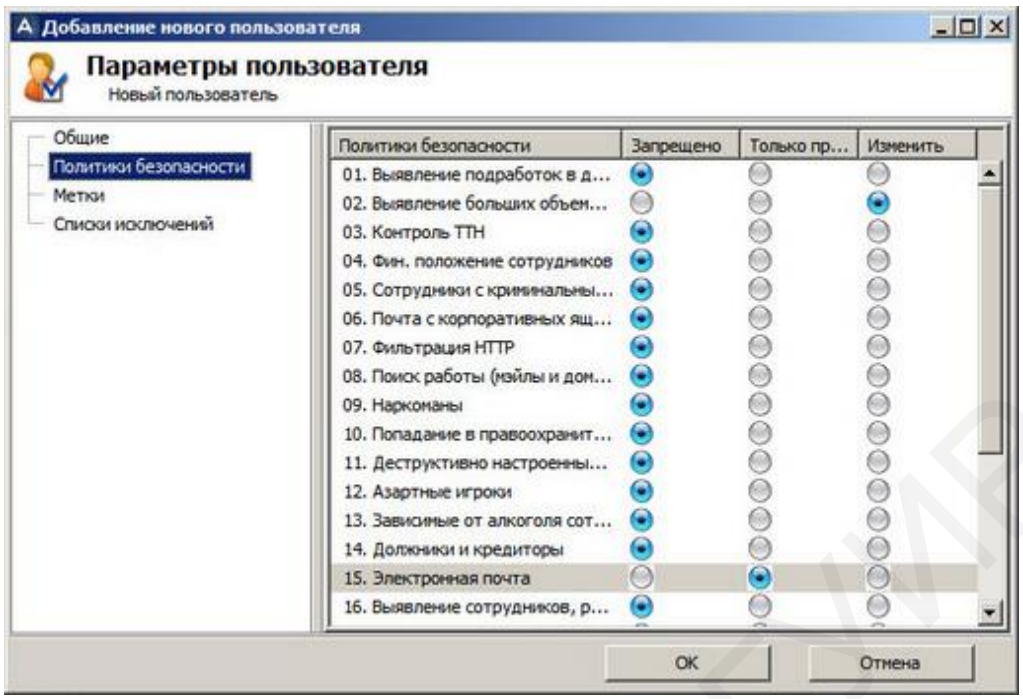


Рис. 3.50. Вкладка «Политики безопасности»

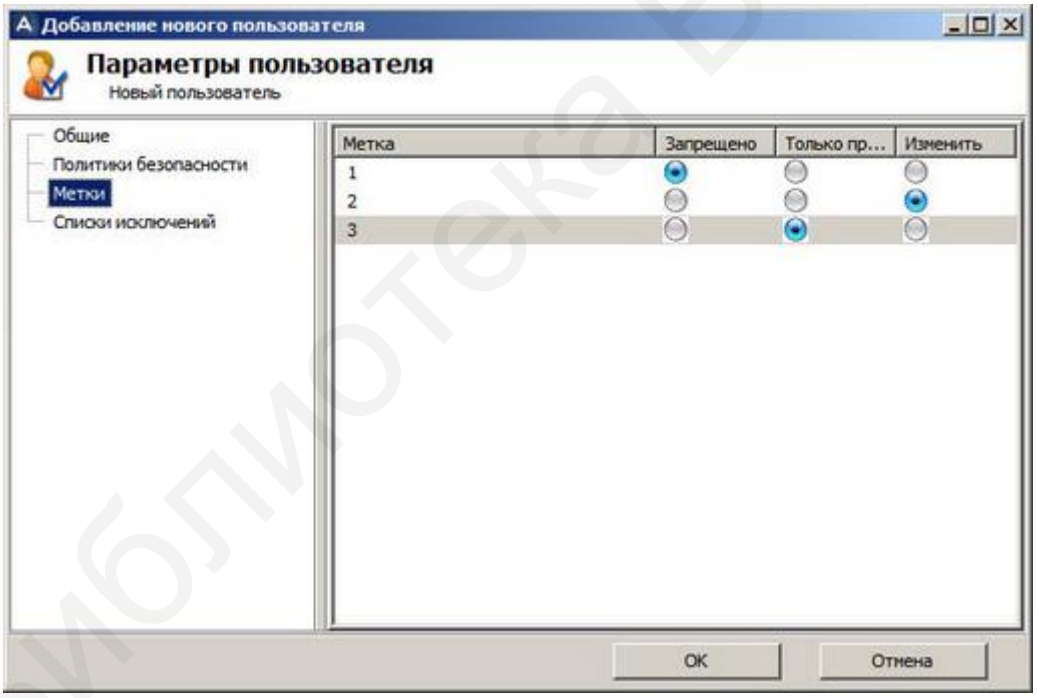


Рис. 3.51. Вкладка «Метки»

Библиотека БГУИР

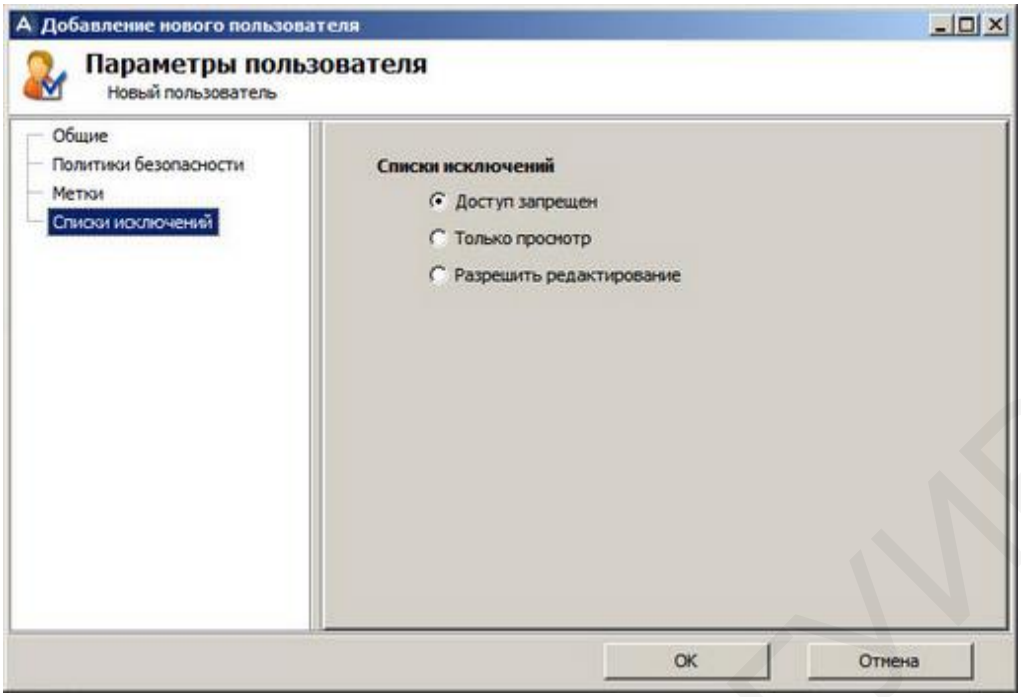


Рис. 3.52. Вкладка «Списки исключений»

По умолчанию для системной учетной записи DefaultAdmin установлено значение «Разрешить редактирование». По завершении настроек всех параметров необходимо нажать кнопку «ОК».

Настройки политик безопасности. Сформированная политика представляет собой набор специфических правил контентного анализа, применяемых в отношении выбранных индексов и баз данных, с учетом расписаний, списков исключений и получателей уведомлений о фактах нарушения данной политики. Политика безопасности формируется на основе одного или нескольких критериев поиска (поисковых запросов), которые настраиваются пользователем.

В списке текущих политик безопасности, который отображается в узле «Политики безопасности» на вкладке «Параметры политики безопасности», предусмотрена возможность выбора даты, начиная с которой будет проверяться действие указанной политики, а также возможность просмотра учетной записи создателя той или иной политики (рис. 3.53).

Для каждой политики можно задать правила доступа к ней пользователей, используя кнопку «Права доступа»:

– «Запрещено» – пользователю недоступны как сама политика, так и результаты проверки по ней;

– «Только просмотр» – пользователь имеет доступ к политике, но без права ее изменения;

– «Изменить» – доступ с правом редактирования.

Библиотека БГУИР

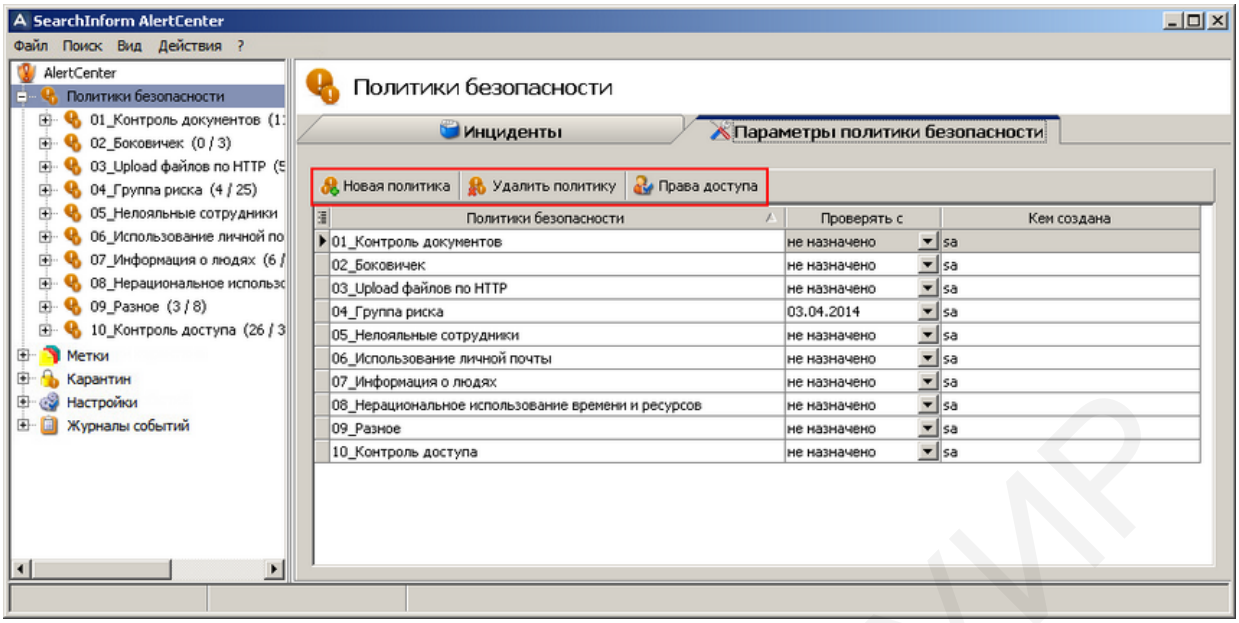


Рис. 3.53. Политики безопасности

Для создания новой политики необходимо выделить узел «Политики безопасности», нажать кнопку «Новая политика», ввести имя политики и подтвердить его нажатием «OK» (рис. 3.54). Затем следует выделить созданную группу и настроить в ней следующие позиции (рис. 3.55):

– список критериев поиска;
– перечень проверки;
– расписание проверок;
– список получателей уведомлений;
– списки исключений.

Перечень проверки, список получателей уведомлений и списки исключений можно настроить индивидуально для каждого отдельного критерия поиска.

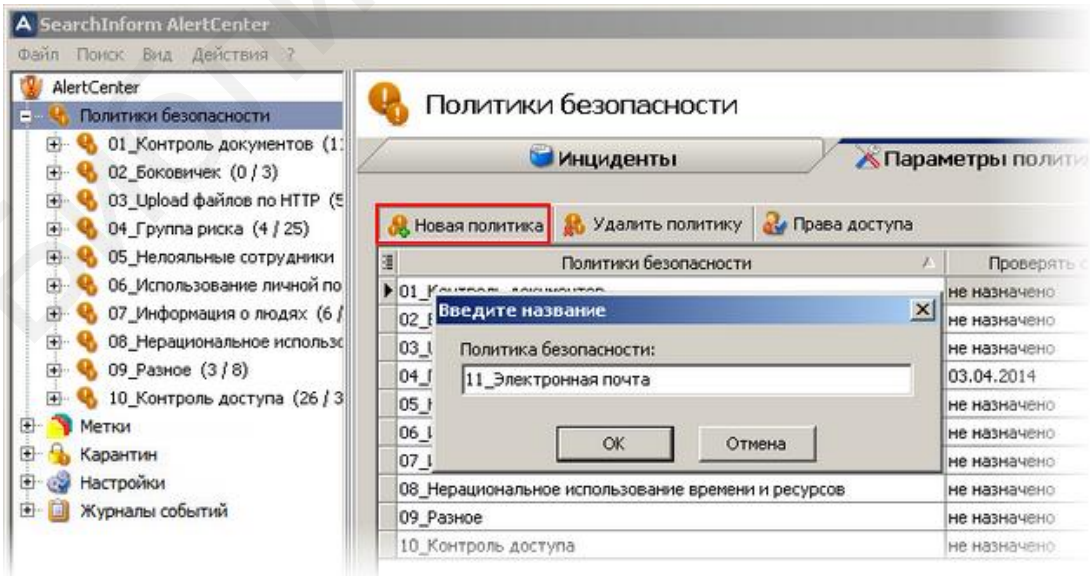


Рис. 3.54. Создание новой политики безопасности

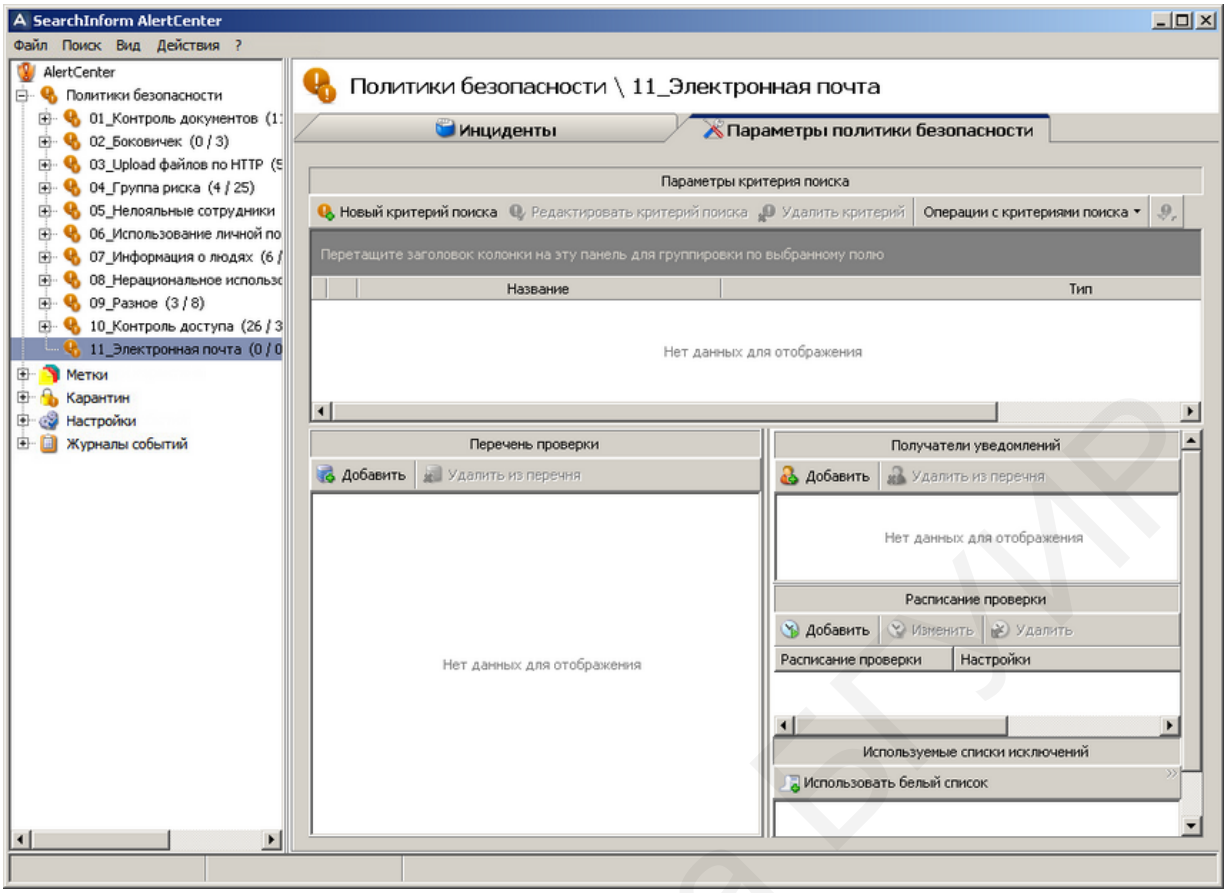


Рис. 3.55. Настройка новой политики безопасности

Настройка критериев поиска. Для нахождения содержащих критичную информацию документов используются поисковые запросы, именуемые критериями поиска. Для добавления запроса предназначена кнопка «Новый критерий поиска». В левой части открывшегося окна необходимо выбрать тип поиска.

Выделяются следующие типы поиска:

– сложные запросы с комбинированием нескольких простых запросов (предъявляется первым по умолчанию);

– фразовый поиск (объединяет возможности поиска по ключевым словам и по фразам);

– поиск по словарю;

– поиск похожих документов;

– поиск по атрибутам документов;

– поиск нераспознанных документов;

– запросы с использованием регулярных выражений;

– запросы с использованием цифровых отпечатков;

– поиск по базам данных;

– запросы Active Directory.

В верхней части окна следует ввести название критерия поиска и (если необходимо) комментарий к нему. Для ограничения периода времени создания документов, соответствующих данному критерию поиска, предназначен флажок в строке «Искать в документах не старше … дней», где указывается количество

дней до текущей даты. Необходимо иметь в виду, что при поиске по индексу локальных файлов и индексам рабочих станций сети параметр «Искать в документах не старше … дней» действует специфическим образом: в результаты поиска попадут файлы, созданные либо модифицированные в течение заданного периода (в зависимости от того, какая дата более поздняя – дата создания или дата изменения).

Затем можно задать другие параметры критерия поиска (в зависимости от выбранного типа) и нажать кнопку «Добавить».

В качестве примера рассмотрим совместное использование фразового поиска и поиска по атрибутам в сложном запросе (рис. 3.56).

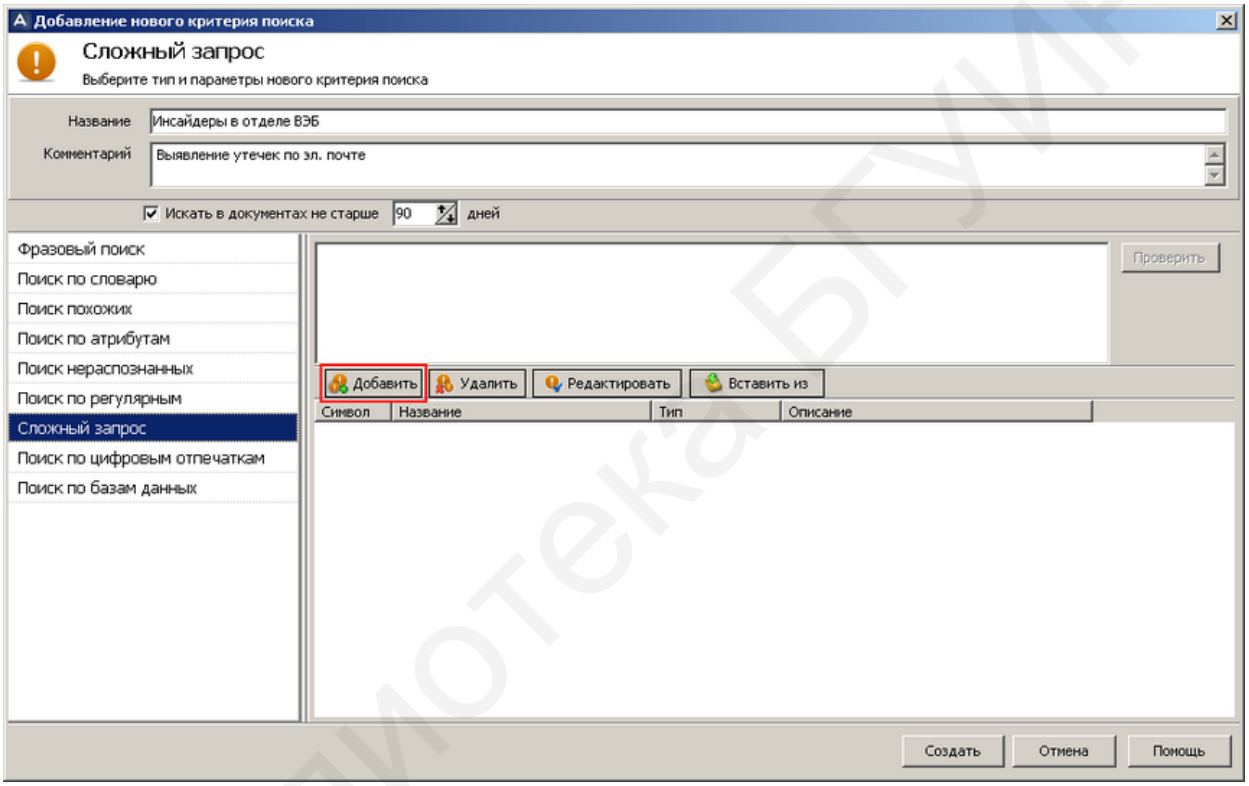


Рис. 3.56. Начало формирования сложного запроса

Введем в качестве названия в одноименное поле фразу «Инсайдеры в отделе ВЭД», а в качестве комментария – «Выявление утечек по эл. почте», после чего нажмем «Добавить». В левой части нового окна выберем «Фразовый поиск» и присвоим название «Ключевые фразы» соответствующему простому запросу (рис. 3.57). В поле, предназначенное для формулировки поискового запроса, поместим фразы «не для посторонних ушей, скажу тебе по секрету, главное молчи». Если слова поискового запроса вводятся через запятую, то они обрабатываются как автономные запросы (функция логического оператора OR). Если хотя бы по одному из них обнаружится совпадение, по документу произойдет так называемая «сработка». Активируем настройки «Поиск с морфологией» и «Поиск фразы» с числом промежуточных слов, равным 2. Нажмем «Создать».

Библиотека БГУИР

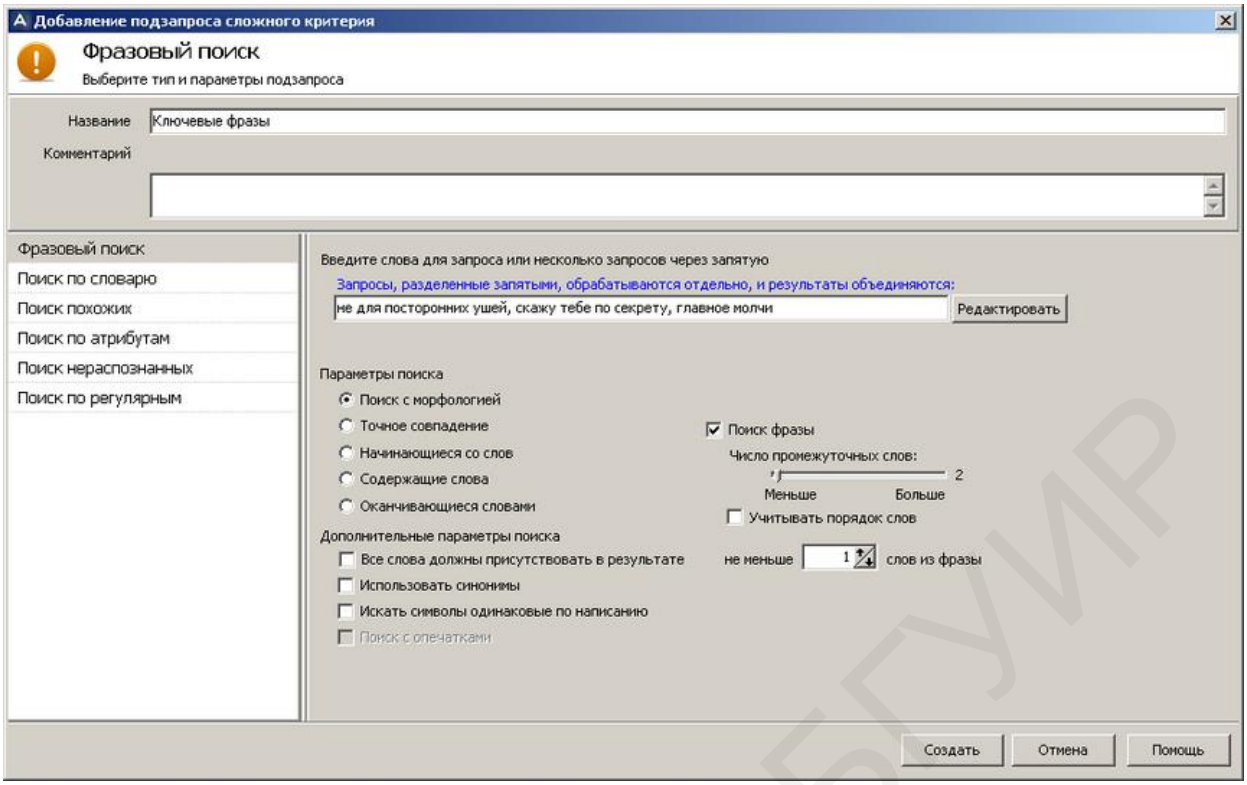


Рис. 3.57. Настройка параметров фразового поиска

Добавим еще один простой запрос, выбрав на этот раз «Поиск по атрибутам» (рис. 3.58).

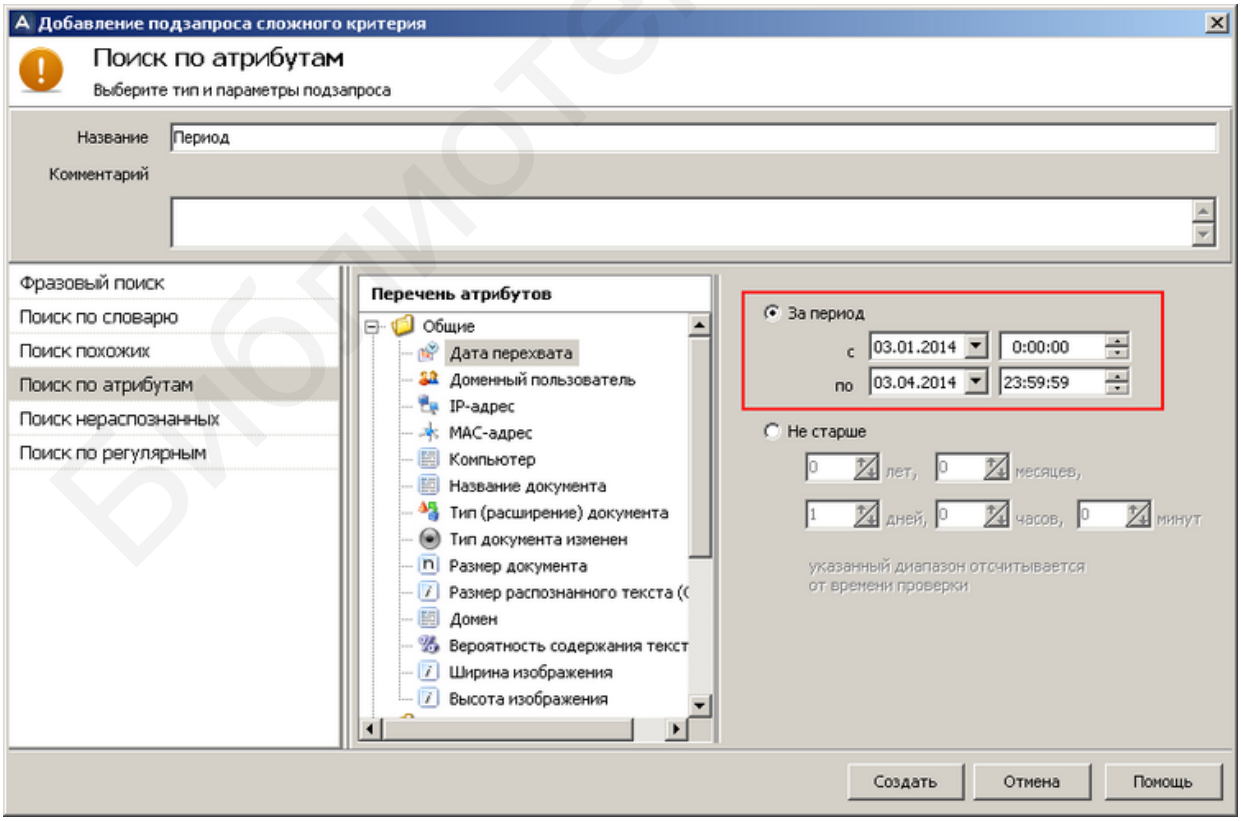


Рис. 3.58. Настройка параметров поиска по атрибутам

Библиотека БГУИР

В перечне атрибутов в разделе «Общие» выберем «Дата перехвата» и справа в блоке «За период», установим требуемые значения «с 00:00:00 03.01.2014 по 23:59:59 03.04.2014». Нажмем «Создать». Используем формулу «A and B» (рис. 3.59) и снова нажмем «Создать». В результате добавленный сложный запрос отобразится в окне «Параметры критерия поиска» (рис. 3.60).

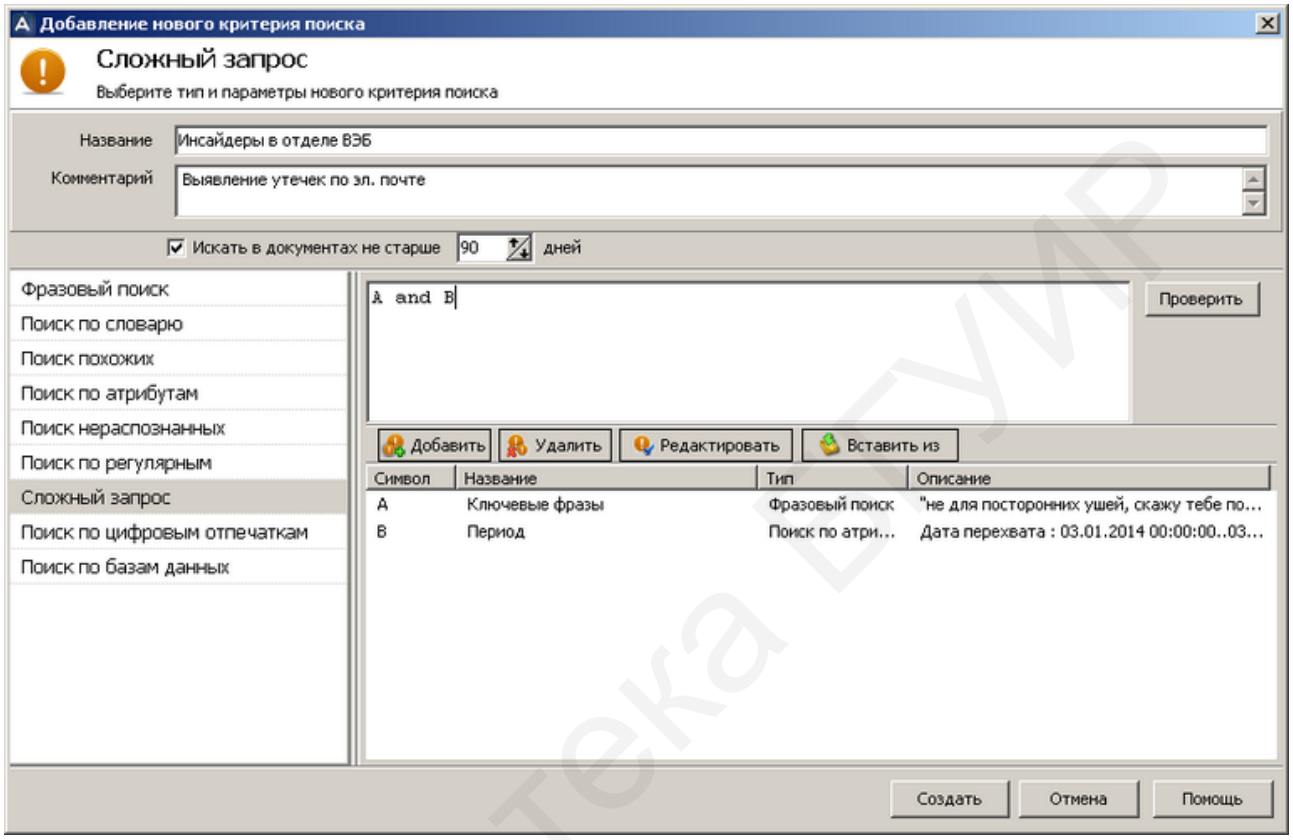


Рис. 3.59. Добавление нового критерия поиска по сложному запросу

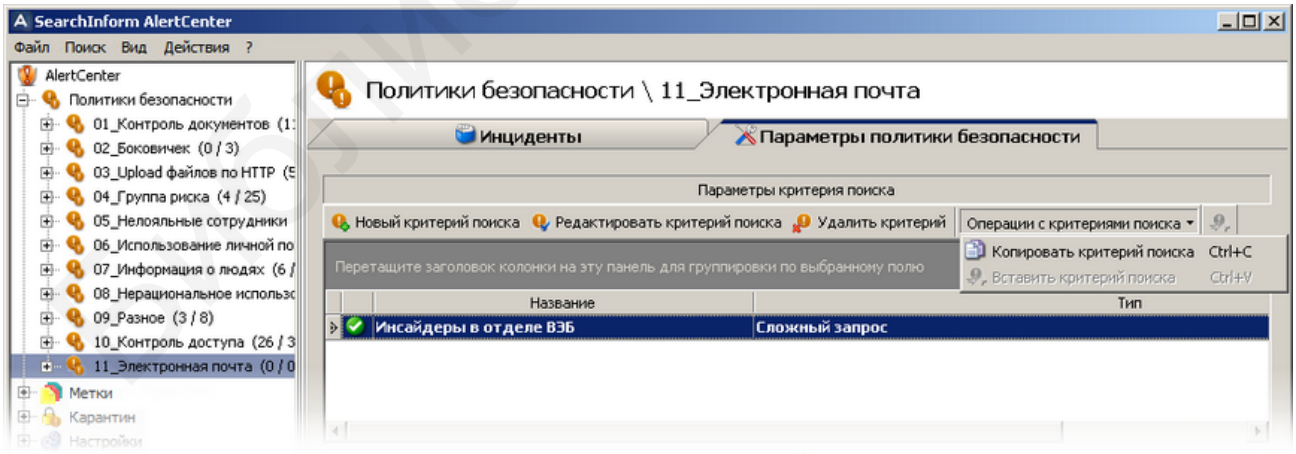


Рис. 3.60. Внешний вид окна с результатами выполнения поиска по сложному запросу

Редактирование запроса производится при помощи кнопки «Редактировать критерий поиска», а удаление – при помощи кнопки «Удалить критерий». Критерий поиска можно скопировать в буфер обмена и вставить в другую по-

Библиотека БГУИР

литику при помощи кнопки «Операции с критериями поиска». Все кнопки дублируются в контекстном меню, вызываемом щелчком правой кнопки мыши.

Настройка индексов для анализа. Для редактирования перечня индексов, по которым будет производиться проверка, следует воспользоваться кнопкой «Изменить» (рис. 3.61) в блоке дополнительных настроек «Перечень проверки».

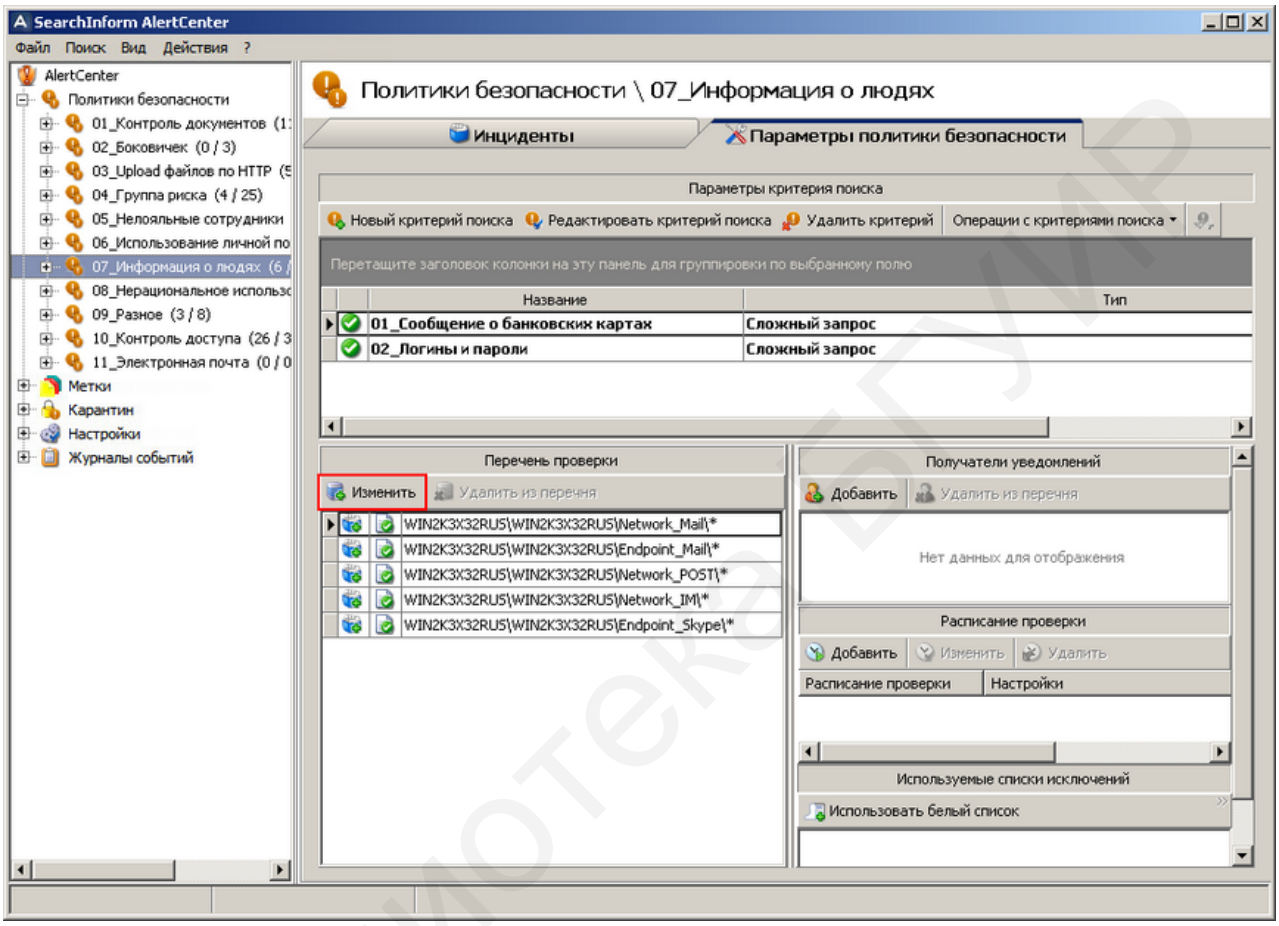


Рис. 3.61. Редактирование перечня индексов,
по которым будет производиться проверка

В открывшемся диалоговом окне отметьте один или более индексов/баз данных. Для выбора ВСЕХ индексов/баз данных, имеющихся на сервере, установите флажок напротив имени сервера. Параметр «Сейчас выбрано» показывает количество выбранных отдельных элементов – серверов, продуктов, цепочек, индексов и баз данных (рис. 3.62).

Библиотека БГУИР

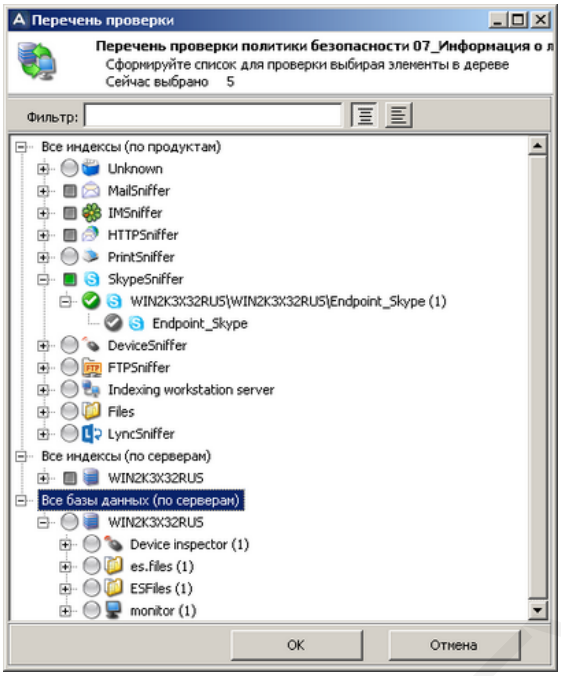


Рис. 3.62. Выбор индексов, по которым будет производиться проверка

Настройка расписания проверок. Расписание определяет, с какой частотой происходит проверка индексов перехваченных документов. Соответствующая настройка производится в разделе «Дополнительные настройки» для выбранной политики безопасности. Для настройки расписания необходимо воспользоваться кнопкой «Добавить» (рис. 3.63) и следовать шагам мастера настройки расписания.

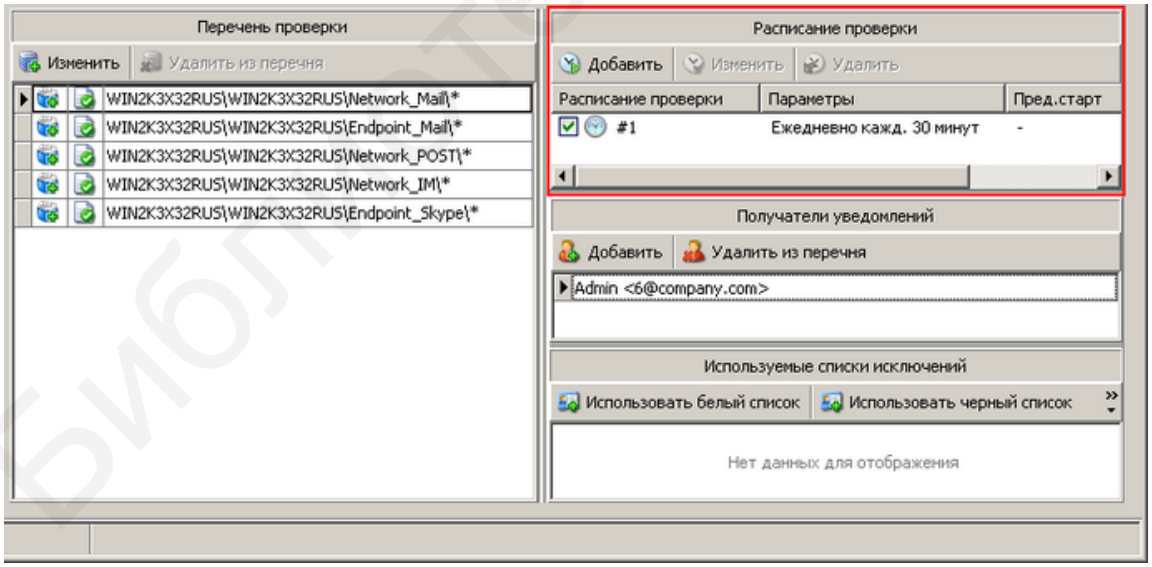


Рис. 3.63. Настройка расписания проверки

Настройка списка получателей уведомлений. При помощи кнопки «Добавить» в группу получателей уведомлений можно добавить только предварительно зарегистрированных пользователей (рис. 3.64).

Библиотека БГУИР

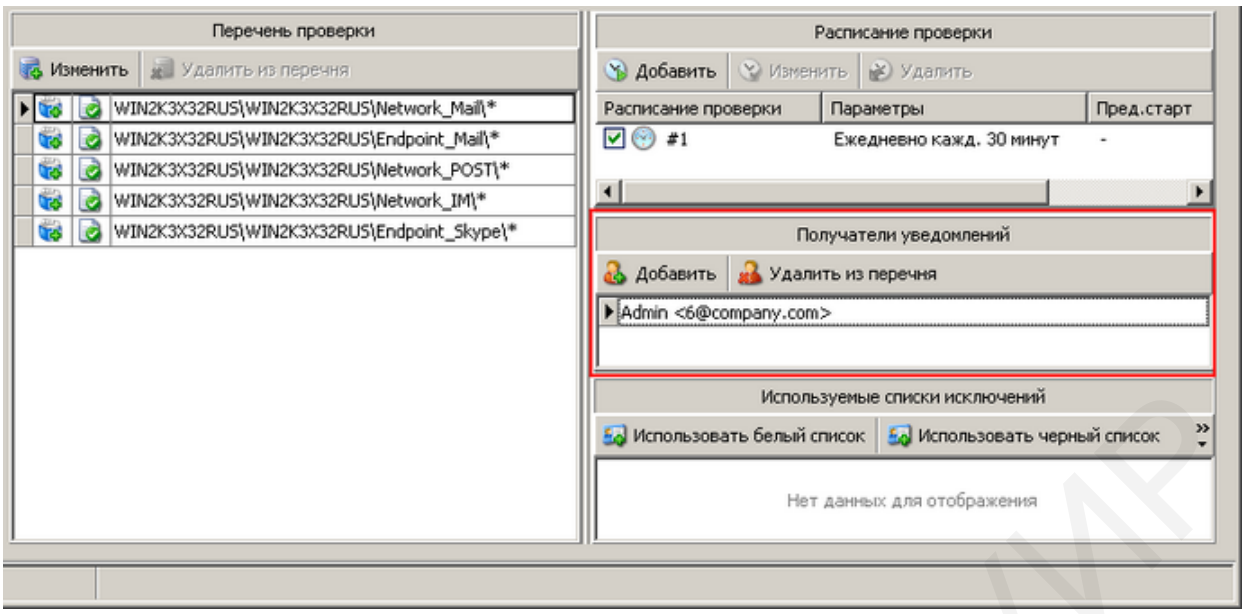


Рис. 3.64. Настройка списка получателей уведомлений

Настройка списка исключений. В зависимости от используемого типа списка либо не будут фиксироваться инциденты по документам пользователей и отправляться уведомления («белый список»), либо, напротив, только по документам заданных пользователей будут фиксироваться инциденты и отправляться уведомления («черный список»). В список исключений можно добавить только имеющихся в общем списке исключений пользователей. Для этого следует нажать кнопку «Использовать белый список» или «Использовать черный список» (рис. 3.65) и выбрать требуемые группы пользователей из общего списка. Для каждой политики можно выбрать только один из типов списков – либо «белый», либо «черный». Например, если уже выбран «белый список», то к нему можно добавить только другие «белые», а вот «черные» добавить уже не получится. Для удаления списка необходимо использовать кнопку «Удалить из перечня».

Существует возможность задать индивидуальные параметры для каждого из критериев поиска. Перейдите в узле «Политики безопасности» на требуемую политику безопасности, выделите нужный критерий. Установите флажок в строке «Разрешить индивидуальные настройки для этого критерия» (рис. 3.66).

Настройки для отдельного критерия поиска аналогичны настройкам для политики безопасности (перечень проверки, получатели уведомлений, используемые списки исключений). Исключение – параметр «Расписание проверки», который является общим для всех критериев поиска в рамках одной политики безопасности.

Библиотека БГУИР

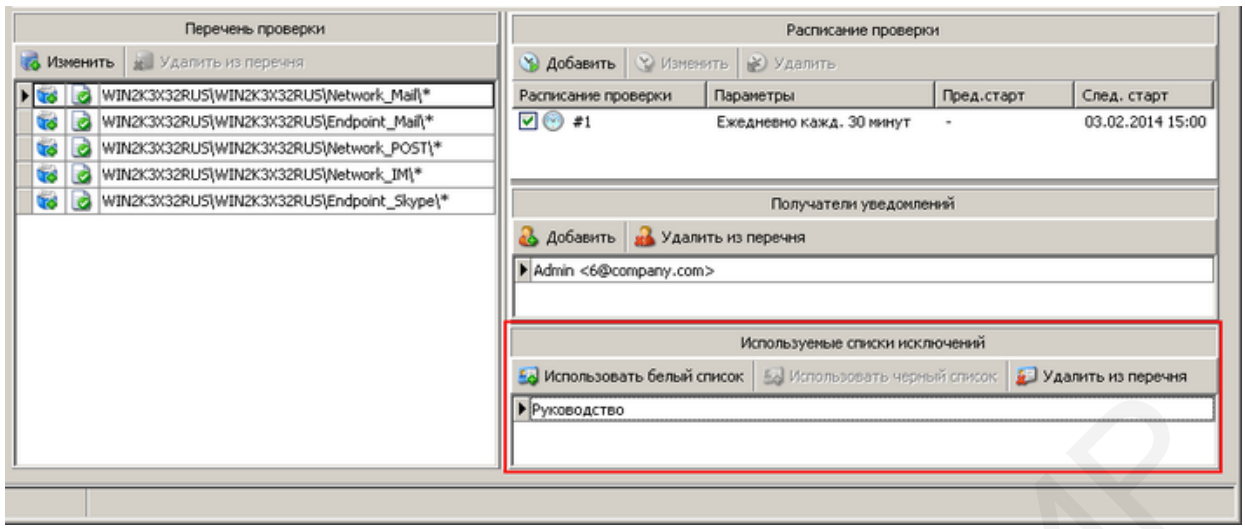


Рис. 3.65. Настройка списка получателей уведомлений

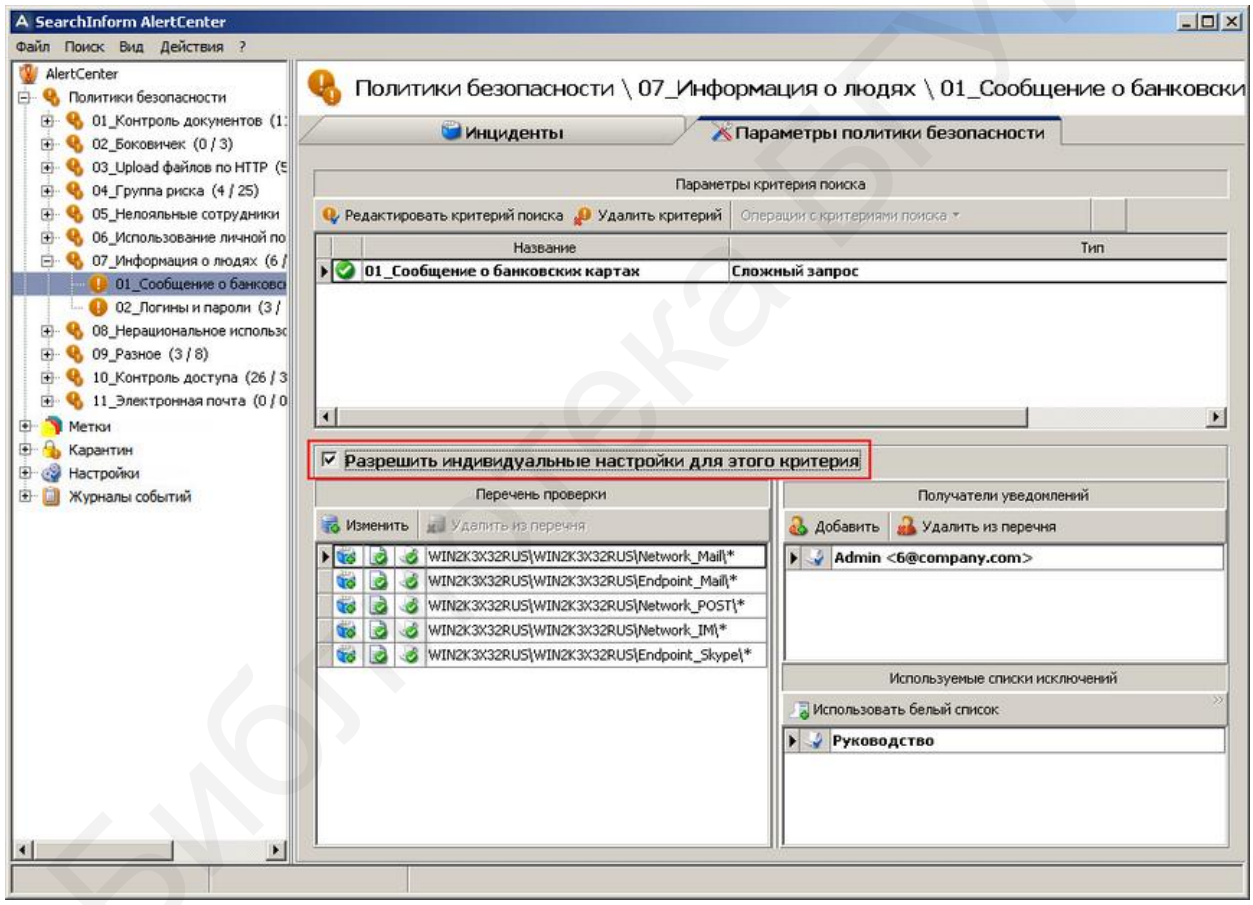


Рис. 3.66. Индивидуальные настройки критерия

После завершения всех настроек процедуру проверки можно запустить вручную, выбрав соответствующую команду в контекстном меню (рис. 3.67).

Библиотека БГУИР

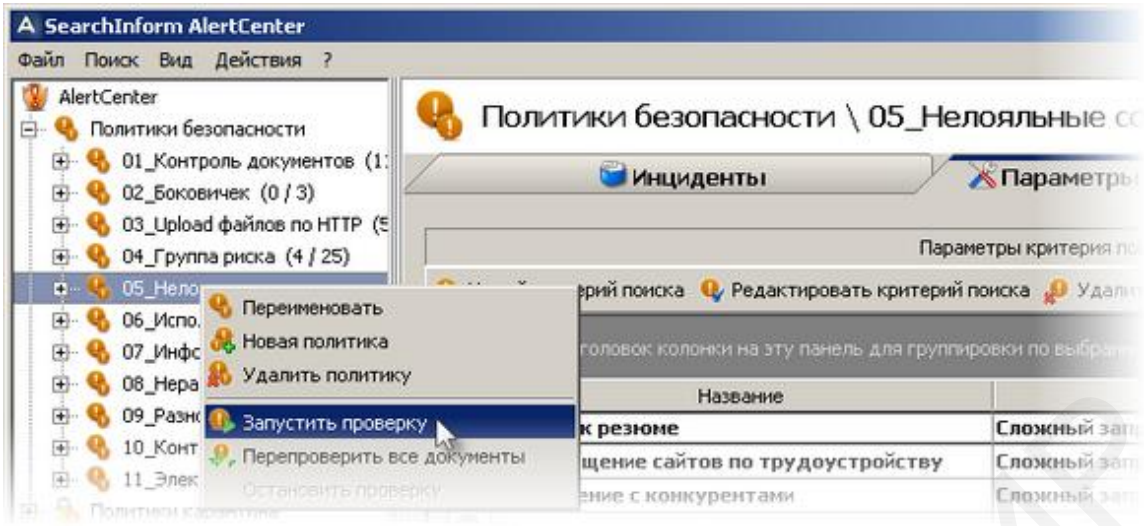


Рис. 3.67. Запуск процедуры проверки

Управление журналом инцидентов. Все срабатывания сервера сохраняются в журнал инцидентов AlertCenter вне зависимости от того, отправлено почтовое уведомление или нет. Работу с инцидентами можно производить как по ссылкам из отправленных по электронной почте уведомлений, так и в журнале результатов. Журнал инцидентов включает в себя документы, по которым сработали поисковые запросы текущей базы AlertCenter. Для просмотра журнала инцидентов следует выделить узел «Инциденты» (рис. 3.68).

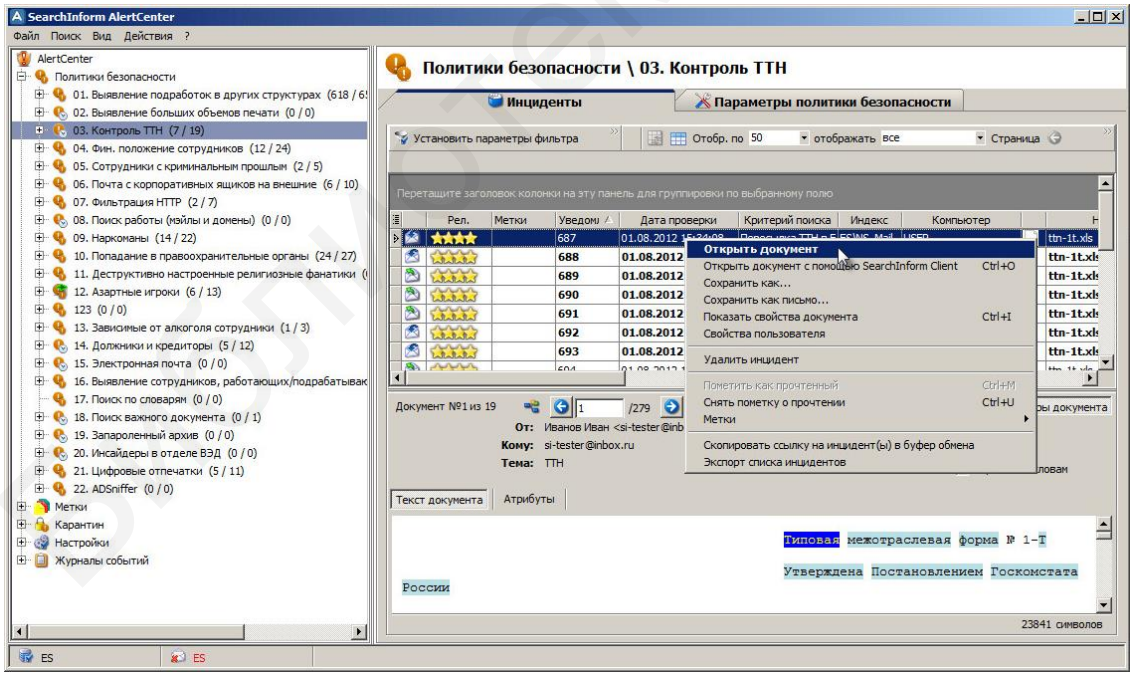


Рис. 3.68. Управление журналом инцидентов

Информация в журнале инцидентов группируется по политикам и критериям поиска (поисковым запросам). Документы, по которым сработали критерии поиска, отображаются в виде списка в правой верхней части окна.

С помощью кнопок, расположенных на панели инструментов, можно производить операции по фильтрации документов, задавать ограничения по количеству отображаемых в списке документов, отображать только непрочитанные сообщения либо только документы, на которые следует обратить внимание. Для изменения количества отображаемых в списке документов можно воспользоваться выпадающим списком в поле «Отбор по…». Для изменения количества отображаемых на странице документов воспользуйтесь выпадающим списком «Отобр. по», для выбора режима отображения сообщений – выпадающим списком «отображать»:

– «все» – отображаются все сообщения;

– «непрочитанные» – отображаются только непрочитанные сообщения;

– «помеченные» – отображаются только сообщения с метками (сообщения можно группировать по отдельным меткам).

Параметры инцидента (или нескольких инцидентов, если выделено более одного) можно скопировать в буфер обмена с помощью клавиш Ctrl+C.

В правой нижней части окна отображается содержимое выделенного документа, при множественном выборе – последний из выделенных документов.

Для отображения атрибутов документа следует воспользоваться кнопкой «Параметры документа». При нажатой кнопке «Параметры документа» отображается кнопка-флажок в строке «Перенос по словам». При снятом флажке перенос строк не производится, навигация по содержимому документа осуществляется с помощью полосы горизонтальной прокрутки. Перенос по словам ограничен размером текста, равным 100 КБ либо 102 400 символам (100×1024). Если указанные параметры превышены, AlertCenter не будет выполнять перенос строк по словам

Щелчком правой кнопки мыши по любому из документов в списке открывается меню, содержащее следующие команды:

– «Открыть документ»;

– «Открыть документ с помощью SearchInform Client»;

– «Сохранить как…»;

– «Показать свойства документа»;

– «Свойства пользователя»;

– «Удалить инцидент»;

– «Пометить как прочтенный»;

– «Снять пометку о прочтении»;

– «Метки»;

– «Экспорт списка инцидентов в HTML».

Для открытия в сопоставленном операционной системой приложении документа, по которому произошла «сработка», можно воспользоваться двойным щелчком кнопки мыши по названию документа или выбрать команду «Открыть документ» в контекстном меню.

Для открытия документа в клиентском приложении КИБ необходимо выбрать команду «Открыть документ с помощью SearchInform Client» в контекстном меню или щелкнуть по ссылке, расположенной под списком. Данная

Библиотека ВГУИР

команда недоступна для инцидентов, сгенерированных по документам, запротоколированным сервером индексации SoftInform Search.

Для просмотра параметров перехваченного документа необходимо в контекстном меню выбрать и нажать кнопку «Показать свойства документа». Из окна «Параметры документа» (рис. 3.69) можно скопировать необходимые атрибуты. Для этого следует их выделить и нажать Ctrl+C. Атрибуты будут скопированы в буфер обмена.

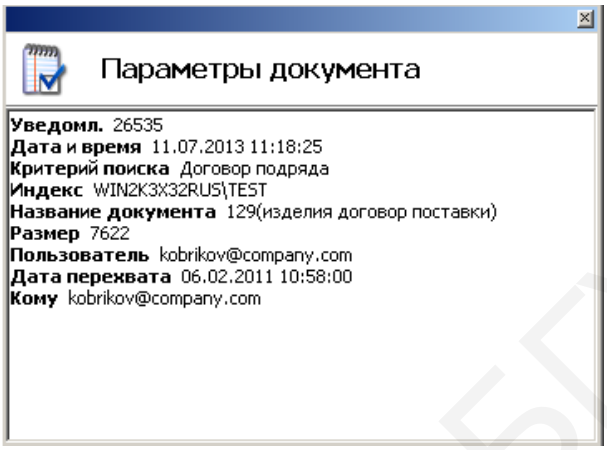


Рис. 3.69. Просмотр параметров перехваченного документа

Просмотр критерия поиска, сработавшего на документе, осуществляется двойным щелчком кнопки мыши по названию критерия в списке.

Список инцидентов можно экспортировать в HTML-файл (рис. 3.70).

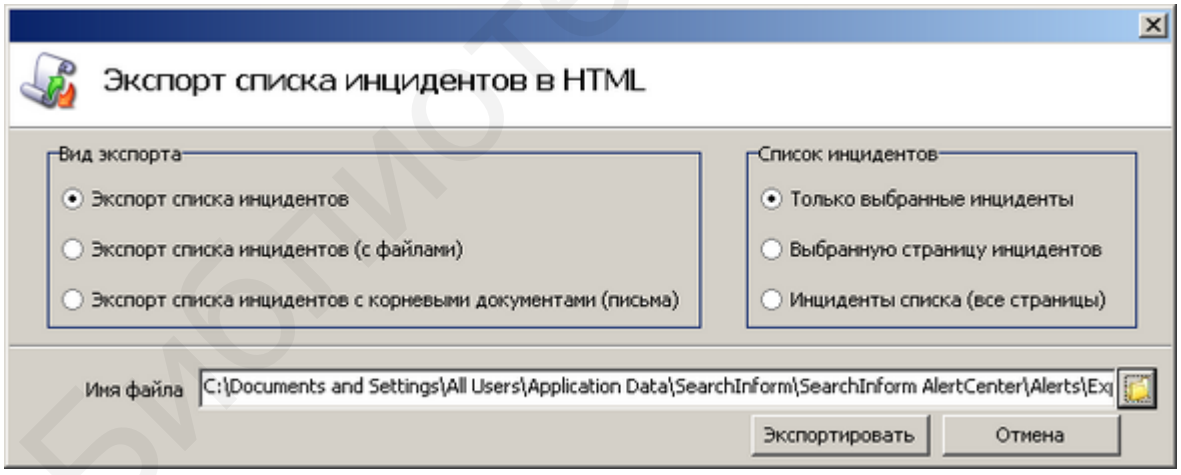


Рис. 3.70. Экспорт инцидентов в HTML

Вызовите контекстное меню и выберите команду «Экспорт списка инцидентов в HTML» или в меню «Действия» – команду «Экспорт списка инцидентов в HTML». Возможны три варианта экспорта:

– экспорт списка инцидентов – будет создан только список инцидентов;

– экспорт списка инцидентов (с файлами) – будет экспортирован список документов со всеми вложенными в него файлами;

Библиотека БГУИР

– экспорт списка инцидентов с корневыми документами (письма) – будет экспортирован список документов вместе с письмами (формат EML).

Задайте необходимые настройки для параметров «Вид экспорта» и «Список инцидентов».

Экспортированный документ можно открыть в веб-браузере.

Если в результате проверок произошло множество срабатываний, журнал инцидентов будет содержать огромное число записей. Поэтому список инцидентов можно *фильтровать*.

Для вызова окна настройки фильтра используется кнопка «Установить параметры фильтра» (рис. 3.71). Записи можно фильтровать:

– по дате и времени фиксации инцидента;

– по дате и времени перехвата;

– по атрибутам.

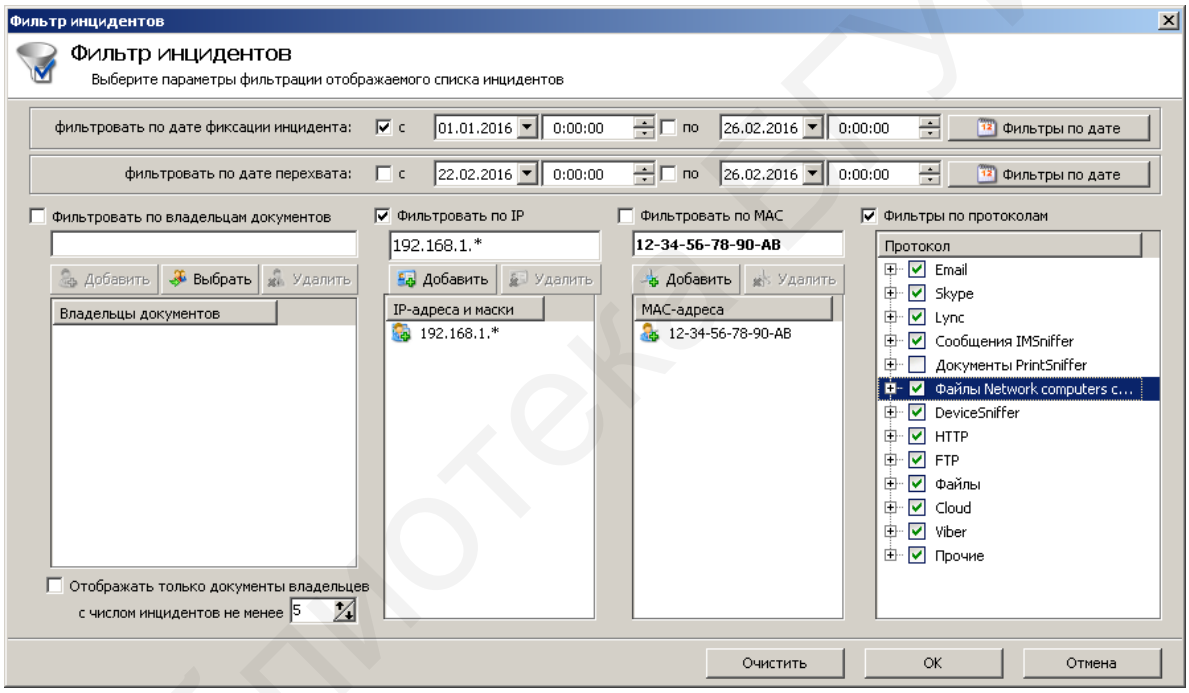


Рис. 3.71. Фильтрация списка инцидентов

Фильтр по дате фиксации инцидента. Для выборки инцидентов по дате и времени фиксации инцидента нужно установить флажок в строке «Фильтровать по дате фиксации инцидента» и настроить требуемый диапазон. Также можно воспользоваться кнопкой «Фильтры по дате».

Фильтр по дате перехвата. Для выборки инцидентов по дате и времени перехвата следует установить флажок в строке «Фильтровать по дате перехвата» и настроить требуемый диапазон либо воспользоваться кнопкой «Фильтры по дате».

Также можно настроить фильтры по атрибутам перехваченных сообщений, а именно:

– пользователям домена, на сообщениях которых сработали запросы;

– IP-адресам отправителей сообщений;

Библиотека БГУИР

– MAC-адресам отправителей сообщений;

– протоколам (при наведении указателя мыши на значок протокола отображается всплывающая подсказка).

Предусмотрена возможность использования фильтра по числу инцидентов на сообщениях отправителя. Каждый из фильтров по атрибутам включается посредством установки соответствующего флажка и нажатия кнопки «Применить».

При одновременном применении фильтров по дате и фильтров по атрибутам сообщений будут выданы только записи с заданными атрибутами, перехваченные за указанный промежуток времени.

Для группировки инцидентов по группам (вне зависимости от соответствующих политик безопасности и критериев поиска) предусмотрены метки.

По аналогии с правами пользователя для политик вводятся права пользователя для тегов (меток).

Раздавать права, добавлять новые метки, менять названия тегов, менять порядок меток и удалять их (в том числе метки с установленными правами «только просмотр») может только администратор. Тег может быть отмечен следующими метками: «невидим», «только для чтения», «полные права (редактирование)».

Если тег невидим, то его нет в дереве тегов данного пользователя, и в списке инцидентов не отображается, что какой-то из инцидентов помечен данным тегом.

Если установлена метка «только для чтения», то пользователь не может снять/поставить данную метку инциденту, но может просматривать инциденты в дереве меток. Производить операции с самим инцидентом пользователь также не может.

При удалении инцидента из политики, а также при очистке списка инцидентов в случае изменения критерия помеченные тегами инциденты не удаляются безвозвратно, а остаются доступными из тегов. В случае снятия метки с инцидента он становится невидим при выборе по данному тегу. При снятии всех тегов с удаленного из политики инцидента он удаляется безвозвратно.

Если пользователь выбирает пункт меню «Удалить инцидент», находясь в тегах, то происходит удаление инцидента из политики с очисткой всех меток текущего инцидента, на которые пользователь имеет право редактирования.

При множественном выделении инцидентов установка меток означает, что всем выделенным инцидентам будут назначены выбранные теги, а все назначенные ранее метки, на которые имеются полные права, снимутся.

Для работы с метками выделите одноименный узел. Щелкните правой кнопкой мыши по узлу и затем нажмите кнопку «Добавить метку» (рис. 3.72).

Библиотека БГУИР

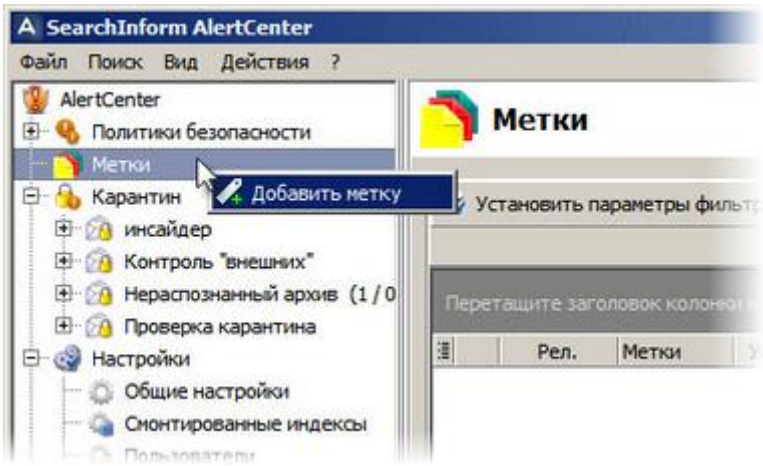


Рис. 3.72. Добавить метку

После добавления необходимых меток перейдите в узел «Политики безопасности» на вкладку «Инциденты». Установите метку для выбранного инцидента с помощью меню, вызываемого правой кнопкой мыши. Метки можно задать из контекстного меню либо с помощью окна, вызываемого командой «Установить метки...» (рис. 3.73).

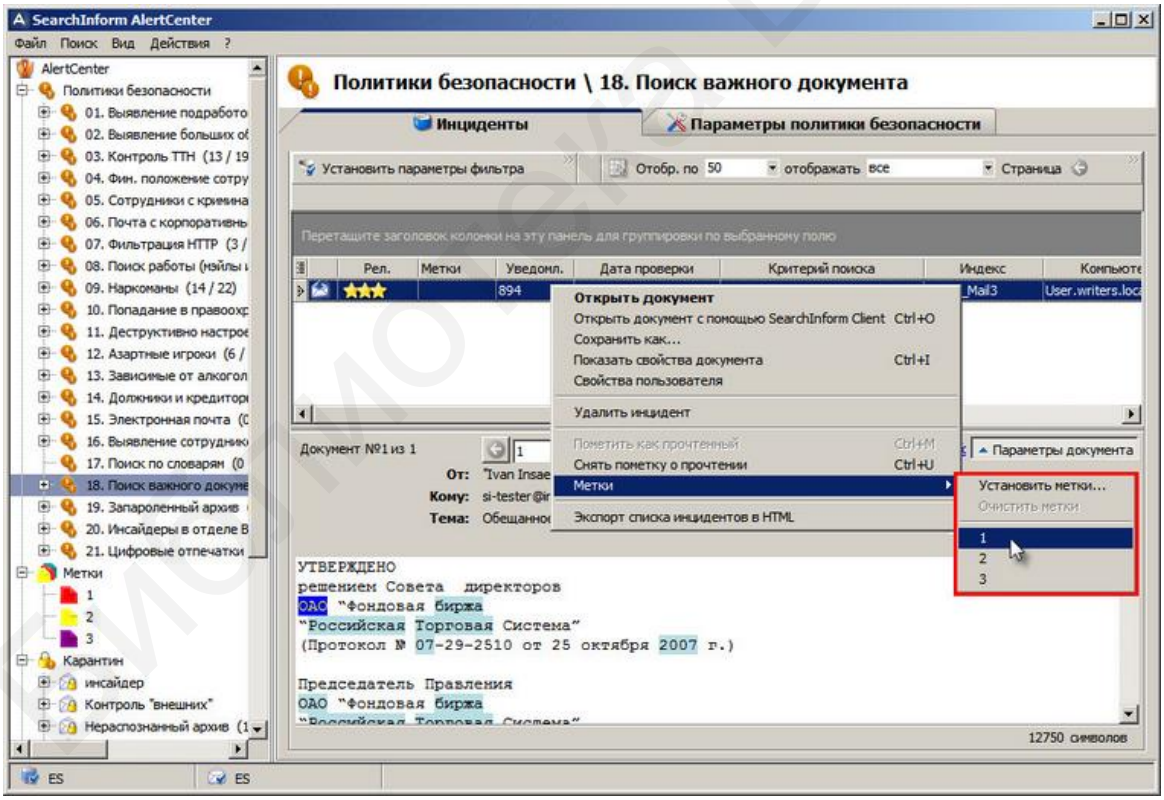


Рис. 3.73. Установка меток

Также метку можно задать инциденту, перетащив его (drag-and-drop) на искомую метку в дереве слева (рис. 3.74).

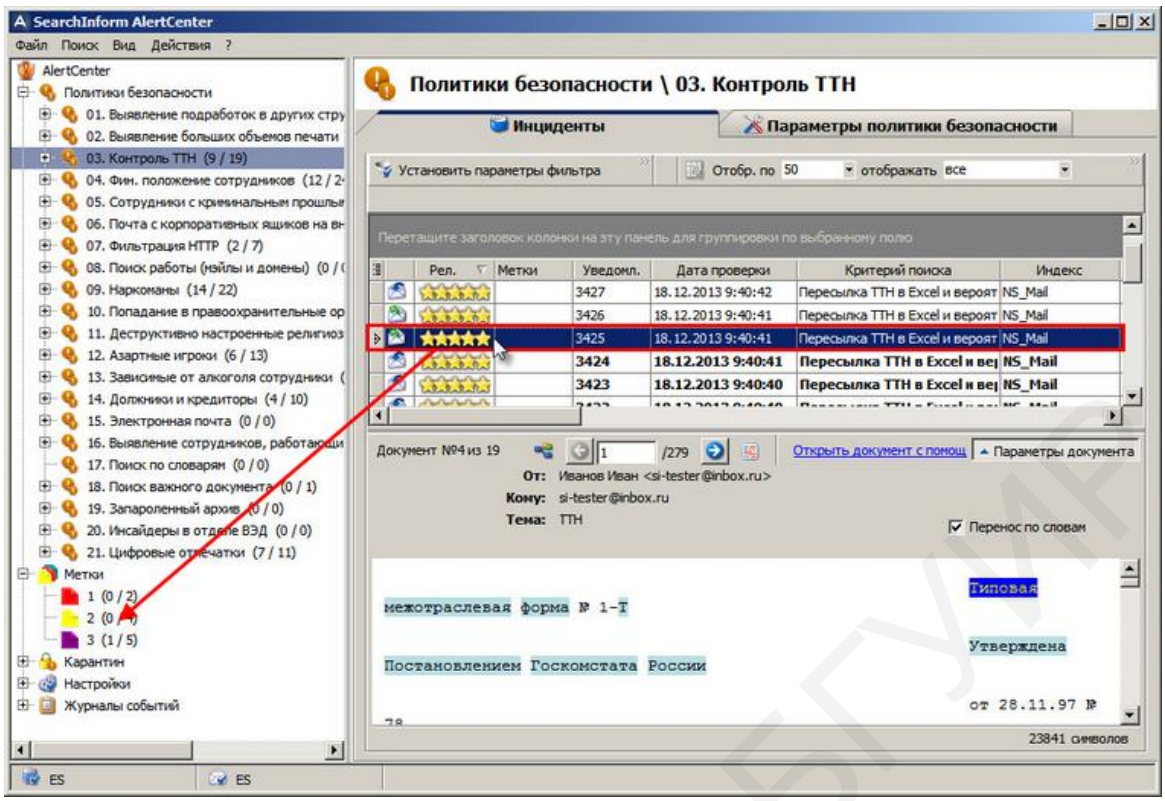


Рис. 3.74. Добавление метки

Одному инциденту могут быть присвоены несколько меток.

После создания политик безопасности при необходимости можно произвести настройку политик карантина. Политики карантина позволяют задать правила для блокирования исходящих сообщений электронной почты, передаваемых по протоколу SMTP. Заблокированные сообщения помещаются в карантин для проведения необходимого анализа их содержания. В дальнейшем в случае отсутствия угрозы сообщения могут быть разблокированы и отправлены по назначению.

Для добавления новой политики следует выделить узел «Карантин» в левой части окна AlertCenter, после чего воспользоваться кнопкой «Новая политика» и ввести имя политики (рис. 3.75).

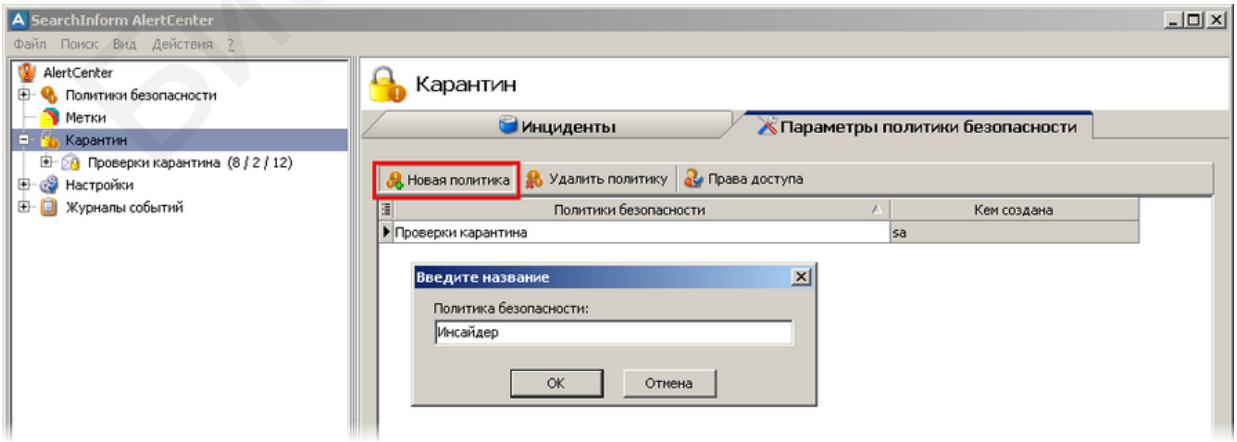


Рис. 3.75. Создание новой политики карантина

Выделив созданную группу, необходимо настроить следующие позиции:
– список критериев поиска;
– перечень проверки (список индексов для анализа);
– общие настройки для карантина (интервал проверки и адрес сервера);
– список получателей уведомлений;
– списки исключений.

Настройка всех перечисленных пунктов, за исключением общих настроек для карантина, осуществляется аналогично тому, как это было рассмотрено применительно к политикам безопасности.

К числу общих настроек для карантина относятся интервал проверки и настройки SMTP-сервера. Для изменения текущих параметров карантина используется кнопка «Изменить» на панели дополнительных настроек. После ее нажатия в соответствующем окне следует ввести необходимые параметры и нажать «OK» (рис. 3.76).

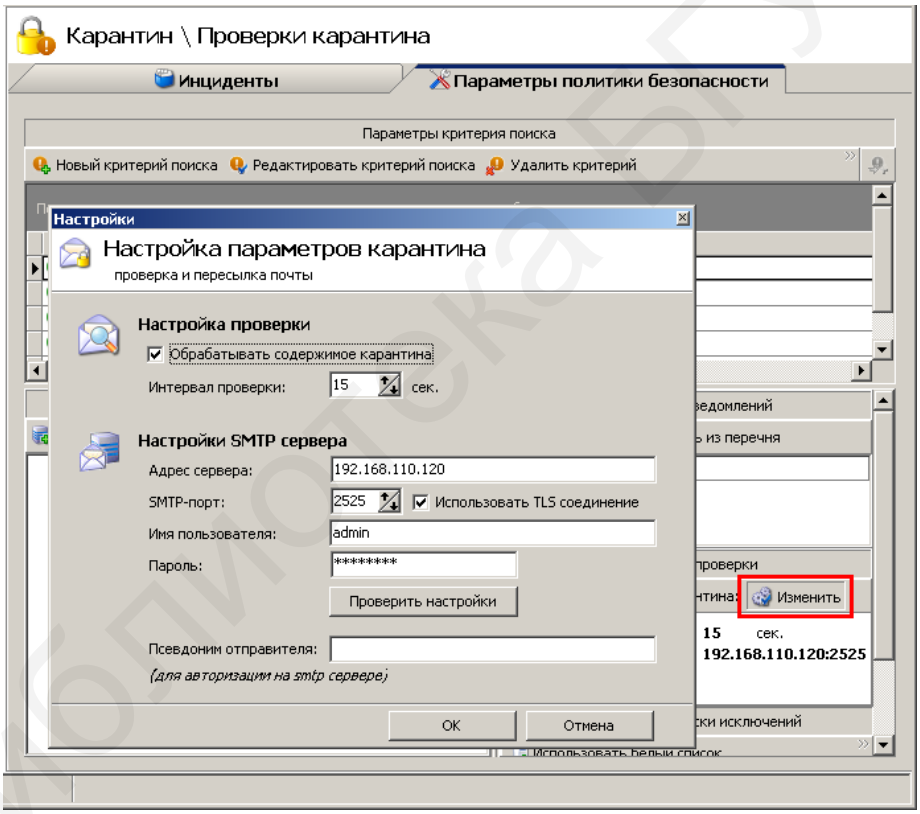


Рис. 3.76. Настройка параметров политики карантина

Клиентская часть AlertCenter позволяет просмотреть результат действия созданных и настроенных политик карантина.

Для просмотра результата нужно выделить узел «Карантин» (рис. 3.77) в левой части окна клиента. При этом в правой части окна отобразится перечень всех перемещенных в карантин сообщений.

Библиотека БГУИР

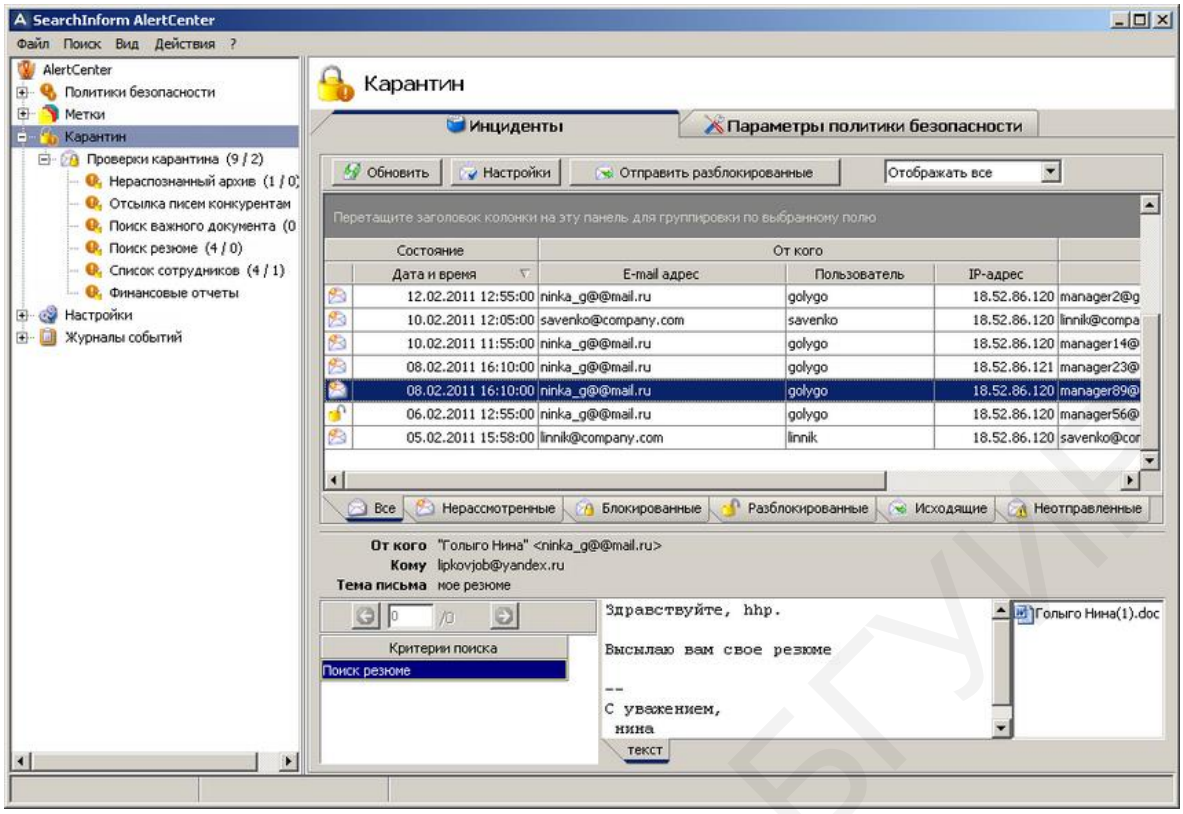


Рис. 3.77. Просмотр результата действия созданных и настроенных политик карантина

В панели со списком помещенных в карантин сообщений отображаются следующие данные:

– категория сообщения (обозначается пиктограммой);
– дата и время отправки письма;
– электронный адрес отправителя сообщения;
– учетная запись отправителя;
– IP-адрес отправителя;
– электронный адрес получателя сообщения;
– IP-адрес получателя;
– номер порта, через который отправлялось сообщение.

Имеется возможность фильтрации помещенных в карантин сообщений по хронологическому критерию:

– указанный период времени;
– весь период;
– сегодня;
– эта неделя;
– этот месяц;
– этот год.

Отображаемая в первой колонке списка пиктограмма указывает на отнесенность сообщения к одной из пяти категорий:

– нерассмотренные (отображаются черным шрифтом);
– блокированные (отображаются красным шрифтом);

Библиотека БГУИР

– разблокированные (отображаются полужирным зеленым шрифтом);

– исходящие (отображаются обычным зеленым шрифтом);

– отправленные (отображаются черным шрифтом).

Сгруппированные по указанным категориям сообщения можно просмотреть с помощью расположенных в нижней части панели вкладок.

Под панелью с перечнем помещенных в карантин сообщений располагается панель просмотра сообщения (наряду с вложенными в него файлами). Сообщение отображается при его выделении в списке верхней панели.

По находящимся в карантине сообщениям может быть принято решение: либо блокировать выбранное сообщение, либо разблокировать, либо отправить разблокированное сообщение на указанный адрес.

Для блокировки-разблокировки выбранных сообщений служат соответствующие команды контекстного меню либо комбинации клавиш:

– Ctrl+B – блокировать сообщение;

– Ctrl+U – разблокировать сообщение.

Отправка разблокированных сообщений производится при помощи кнопки «Отправить разблокированные». Данное действие носит необратимый характер: все разблокированные сообщения на период отправки будут перемещены во вкладку «Исходящие» и в случае успешной отправки покинут карантин.

Письма, находящиеся на вкладке «Неотправленные», можно попробовать отправить повторно либо удалить.

Настраиваемые параметры AlertCenter. Для доступа к настройкам предназначен раздел «Общие настройки» (рис. 3.78) узла «Настройки». В число доступных настроек входят: настройки интерфейса пользователя, настройки сервера.

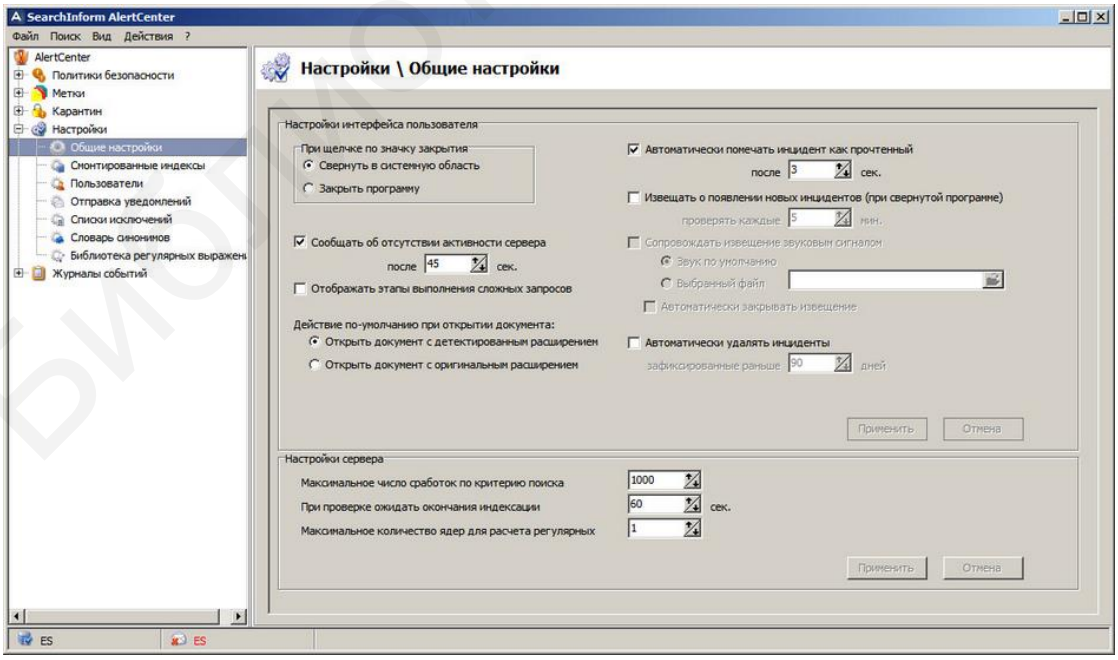


Рис. 3.78. Общие настройки AlertCenter

Библиотека БГУИР

Настройка отправки уведомлений. В случае обнаружения документов согласно условиям поиска AlertCenter должен формировать почтовое сообщение, содержащее ссылки на просмотр документа в клиентских модулях КИБ.

Для настройки параметров отправки уведомлений предназначена вкладка «Отправка уведомлений» в узле «Настройки» (рис. 3.79). Для того чтобы активировать рассматриваемую функцию, необходимо установить флажок в строке «Посылать уведомления по электронной почте» и задать настройки SMTP-сервера:

– «Адрес отправителя»;
– «Адрес сервера»;
– «SMTP-порт»;
– «Имя пользователя»;
– «Пароль».

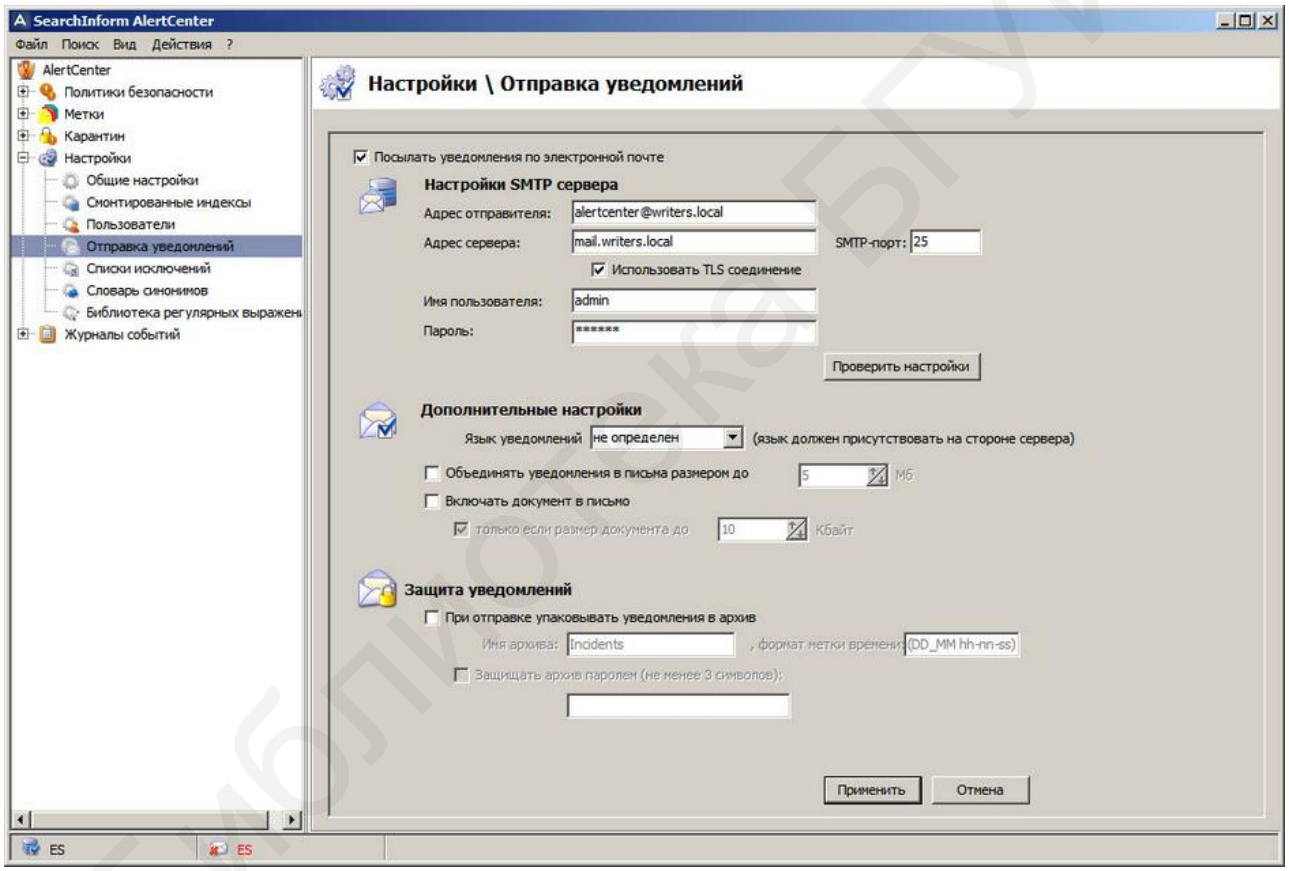


Рис. 3.79. Настройка отправки уведомлений

В случае необходимости использования шифрования при отправке уведомлений необходимо установить флажок в строке «Использовать TLS соединение». Можно использовать также следующие дополнительные настройки:

– «Язык уведомлений» (русский, английский, латышский, польский);

– «Объединять уведомления в письма» – в одном сообщении будут объединены уведомления по всем найденным документам (максимальный размер сообщения настраивается);

Библиотека БГУИР

– «Включать документ в письмо» – для включаемых в уведомление документов может быть настроен максимальный размер в килобайтах.

Также могут быть применены перечисленные далее настройки защиты уведомлений:

– «Упаковка уведомлений в архив при отправке»;

– «Имя архива и формат метки времени»;

– «Защита архива паролем».

Для подтверждения всех настроек по отправке уведомлений следует воспользоваться кнопкой «Применить».

Настройка списков исключений. В список исключений должны быть добавлены группы пользователей, которые в зависимости от типа списка будут:

– либо исключены из зоны применения политик безопасности (так называемый «белый список», включающий пользователей, по документам которых не будут фиксироваться инциденты и отправляться уведомления);

– либо напротив включены в зоны применения политик безопасности (так называемый «черный список», включающий пользователей, по документам которых в обязательном порядке будут фиксироваться инциденты и отправляться уведомления).

Необходимые настройки расположены на вкладке «Списки исключений» узла «Настройки» (рис. 3.80).

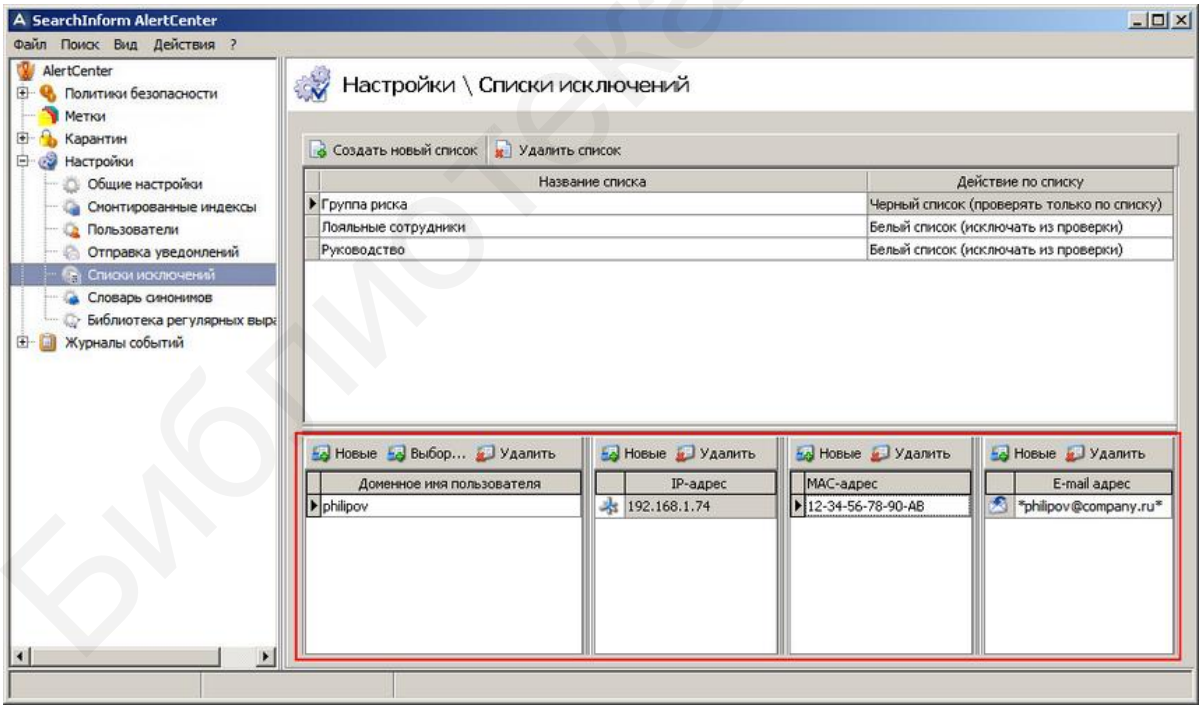


Рис. 3.80. Настройка списков исключений

Для добавления списка следует нажать кнопку «Создать новый список» и ввести имя списка. Имя списка будет добавлено в базу данных. Далее в колонке «Действие по списку» необходимо выбрать тип списка – «белый» либо «черный».

Библиотека БГУИР

Следует помнить, что работать со списками исключений могут только пользователи с установленным правом доступа «Разрешить редактирование».

После добавления списка необходимо ввести параметры исключения пользователей из проверки. Исключение пользователей производится по любому из четырех атрибутов: пользователю домена, IP-адресу, MAC-адресу и адресу электронной почты.

Фильтры по доменным пользователям. При настройке фильтров по именам доменных пользователей используется следующий синтаксис:

– manager – пользователь (любого домена) с доменным именем *manager*;

– domain\manager – пользователь *manager* домена *domain*.

Допускаются маски с использованием оператора * (любая последовательность символов).

Примеры:

– manager* – пользователи, доменные имена которых начинаются на *manager* (*manager, manager123* и т. д);

– domain* – все пользователи домена domain, например, *domain\user123*;

– domain* – все пользователи домена или доменов, начинающихся на *domain*, например, *domain123/user123*;

– *manager (рекомендуемая форма записи, однако иногда при перехвате имя пользователя может формироваться без привязки к домену) или *\manager – пользователь любого домена с именем *manager* (*domain123\manager*);

– *manager* – пользователь (любого домена), имя которого включает manager (*123manager, manager123, 123manager123*);

Оператор * может быть расположен только в начале или конце записи. Образец неправильной записи – domain*\manager.

Фильтры по IP-адресам. В качестве фильтра можно задавать отдельные IP-адреса или маски.

Фильтры по MAC-адресам. В качестве фильтра используется MAC-адрес сетевого адаптера, установленного на компьютере пользователя.

Фильтры по адресам электронной почты. Для адресов электронной почты доступен выбор между получателем и отправителем сообщений.

Словарь синонимов удобно использовать для мониторинга неформального общения сотрудников, выявления тех, кто по каким-либо причинам может быть отнесен к группе риска, а также выявления принадлежности к той или иной профессиональной среде и т. д. Синонимы позволяют задавать максимально широкую область поиска. Примером решения задачи, требующей использования словаря синонимов, может являться поиск прямых или закамуфлированных требований взятки/денег (поиск в переписке различным образом выраженной мысли «хочу взятку»). Для решения указанной задачи в простейшем случае может быть создано два синонимических ряда: для слова, обозначающего желание получить взятку, например, «хочу», синонимами будут «дай», «нужна», «требуется» и т. п., для слова «взятка» – «бакшиш», «бонус»,

Библиотека БГУИР

«гонорар» и им подобные. Синонимы позволят по запросу «хочу взятку» найти все возможные сочетания слов в переписке (например, «нужен бакшиш»). То есть, если ряд 1 включает в себя три слова, а ряд 2 – пять синонимов, то поисковая система проверит все возможные 3·5 = 15 вариантов сочетаний.

Формирование и управление словарями синонимов производится на вкладке «Словарь синонимов» узла «Настройки» (рис. 3.81). Для добавления синонимического ряда используется кнопка «Новая группа». Ввод синонимов осуществляется через запятую, пробел или с новой строки. После нажатия кнопки «ОК» синонимический ряд будет добавлен в словарь.

Следует иметь в виду ряд особенностей применения изменений на поисковом сервере. В процессе поиска сервер SoftInform Search получает синонимы не из базы индексов, а из внутреннего ресурсного файла. При обновлении словаря синонимов обновление ресурсного файла синонимов производится одним из двух вариантов:

– автоматически при переходе на новую вкладку клиента AlertCenter;

– после нажатия кнопки «Применить».

Для поиска требующейся синонимической группы используется кнопка «Фильтровать синонимы» (см. рис. 3.81). При помощи кнопки включается фильтрация по фрагменту всех слов, входящих в синонимические ряды. При помощи кнопки осуществляется поиск по первому слову в синонимическом ряду.

Базы синонимов можно экспортировать. Для экспорта существующего набора синонимов необходимо воспользоваться кнопкой «Импорт/экспорт» и выбрать «Экспортировать» в выпадающем меню. Затем необходимо выбрать папку и указать имя сохраняемого файла. Набор синонимов будет экспортирован в файл с расширением SIS.

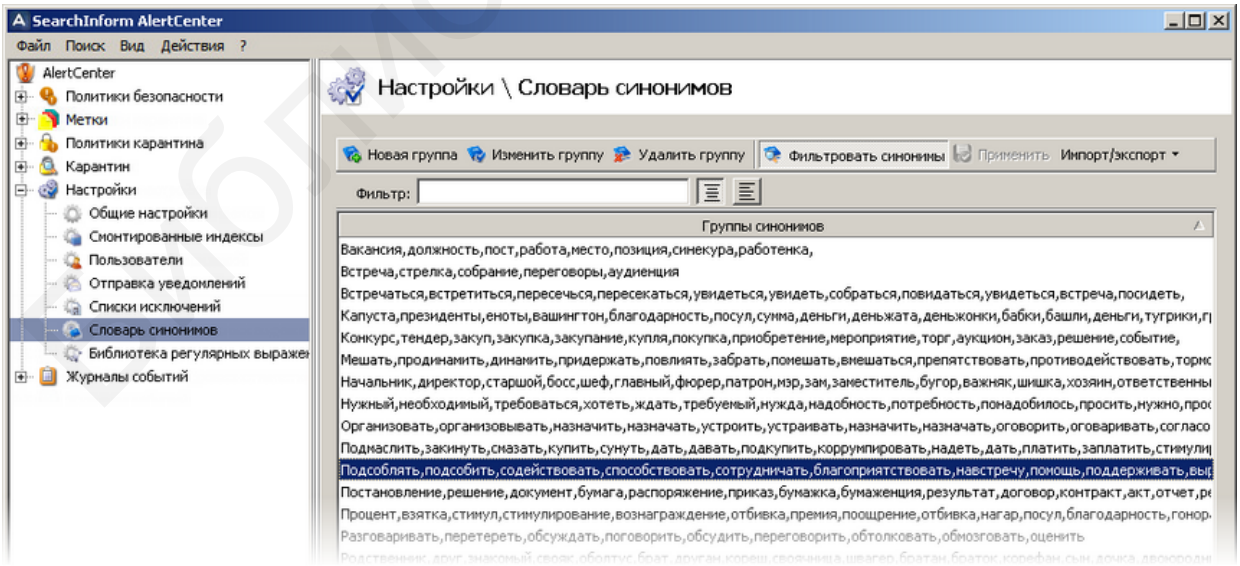


Рис. 3.81. Словарь синонимов

Для импорта файла с набором синонимов следует нажать кнопку «Импорт/экспорт», выбрать команду «Импортировать» в выпадающем меню,

после чего открыть нужную папку и выбрать требуемый файл с расширением SIS. Набор синонимов будет импортирован в базу AlertCenter.

Настройка библиотеки регулярных выражений производится на вкладке «Библиотека регулярных выражений» узла «Настройки» (рис. 3.82).

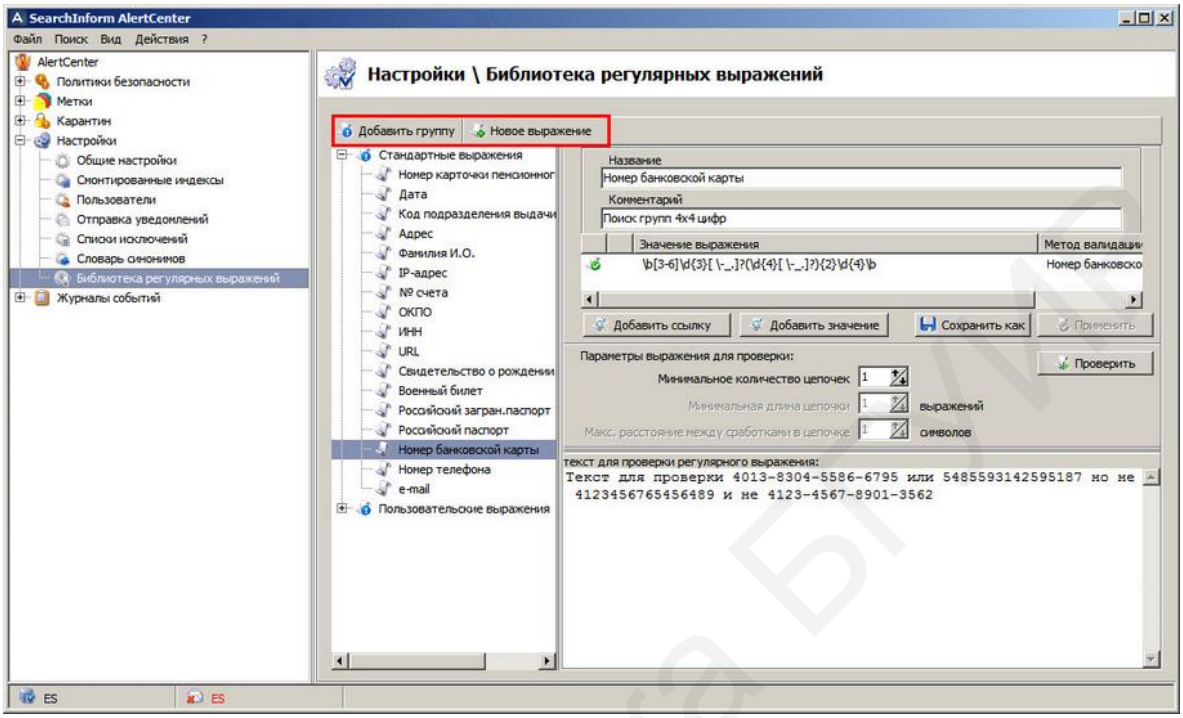


Рис. 3.82. Библиотека регулярных выражений

Библиотека регулярных выражений должна включать в себя:

– шаблоны регулярный выражений, используемые для поиска отдельных элементов текста (например, «номер телефона в международном формате», «номер кредитной карточки», «дата», «номер паспорта» и т. д.);

– составные регулярные выражения или цепочки, которые могут включать в себя два или более шаблонов. В качестве примера можно привести выражение, позволяющее найти документы, содержащие значения «ФИО», «дата рождения», «номер счета», «номер карточки».

Шаблоны регулярных выражений обозначаются значком , составные регулярные выражение – значком . В отличие от обычного шаблона регулярного выражения к числу настраиваемых параметров составного относятся такие, как минимальная длина цепочки, максимальное расстояние между «сработками» в цепочке.

В комплект поставки включено несколько стандартных шаблонов, объединенных в группу «Стандартные выражения», например, «Номер карточки пенсионного страхования», «ОКПО», «ИНН», «Российский паспорт», «Номер телефона» и др. В редактируемом поле колонки «Значение выражения» пользователь может создать и настроить собственный шаблон. Сделанные изменения сохраняются при помощи кнопки «Применить». Шаблоны комбинируются в составные регулярные выражения. Шаблоны и составные регулярные выра-

Библиотека БГУИР

жения могут быть организованы по группам, имя которых задается пользователем. Добавление группы производится при помощи кнопки «Добавить группу». Создание шаблона или сложного составного выражения производится при помощи кнопки «Новое выражение».

В зависимости от типа регулярного выражения для оптимизации поиска выбирается метод валидации. Методы валидации встроены в программу и не могут редактироваться. Метод валидации выбирается из списка: для его открытия необходимо щелкнуть по редактируемому полю в колонке «Метод валидации» (рис. 3.83).

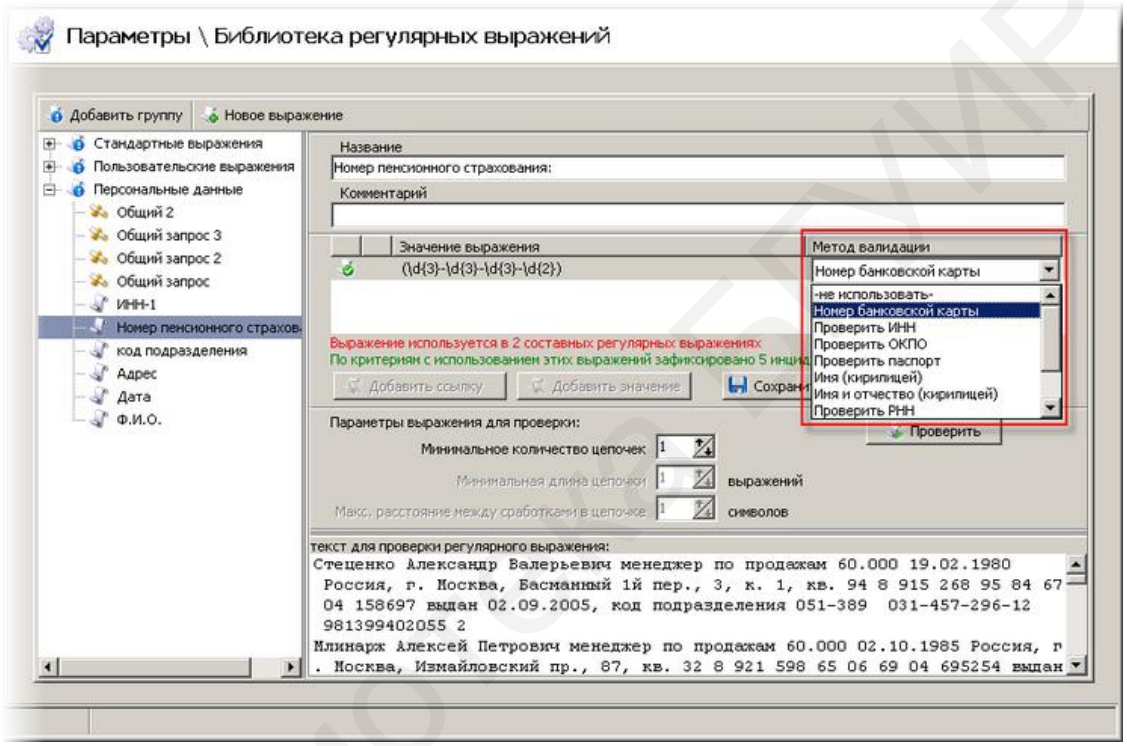


Рис. 3.83. Выбор метода валидации

Введенный шаблон можно проверить. Для этого необходимо ввести текст, по которому будет проверяться выражение, в поле, расположенное в нижней части клиента AlertCenter. Для проверки используется кнопка «Проверить». На тестовом тексте при срабатывании регулярного выражения подсвечивается текст, а справа появляется всплывающее окно с информацией о времени проверки и количестве найденных цепочек. При создании составного регулярного выражения комбинируются несколько шаблонов. Примером может быть поиск списков заказчиков, для организации которого можно использовать пять шаблонов: «юридическая форма», «название организации», «имя контактного лица», «телефон», «адрес электронной почты».

Добавление шаблонов производится при помощи кнопок «Добавить ссылку» и «Добавить значение»:

– использование кнопки «Добавить ссылку» подразумевает, что будет добавлена ссылка на имеющийся шаблон; изменения оригинального шаблона

будут унаследованы и в составном регулярном выражении; при добавлении ссылки будет отображено имя шаблона;

– использование кнопки «Добавить значение» подразумевает, что выбранный шаблон будет импортирован; изменения оригинального шаблона не отразятся на конечном регулярном выражении; при добавлении значения будет отображаться настроенное для шаблона выражение.

Для удаления шаблона регулярного выражения используется кнопка «Удалить выражение» в контекстном меню, вызываемом правой кнопкой мыши. Для поиска по регулярным выражениям сервер AlertCenter должен получить полный текст проиндексированных документов. Поэтому рекомендуется, чтобы для проверяемых по регулярным выражениям индексов была настроена опция «Хранение текстов в индексах». Данную опцию можно включить из клиента AlertCenter. После настройки шаблонов и регулярного выражения необходимо настроить критерий поиска на использование регулярного выражения.

Настройка библиотеки цифровых отпечатков. Для работы с цифровыми отпечатками должна быть сформирована база данных эталонных документов, т. е. тех документов-образцов, с которыми будут сопоставляться перехваченные данные. Подключение/отключение сгруппированных по каталогам образцов осуществляется путем настройки библиотеки цифровых отпечатков. Настройка цифровых отпечатков производится в SearchInform DataCenter. Перейдите на вкладку «Настройки» → «Цифровые отпечатки». В группе настроек «Каталог образцов цифровых отпечатков» задаются папки с образцами. Для настройки расписания индексации цифровых отпечатков используется одноименная кнопка. В нижней части окна задается Search Server, на котором будет создан индекс цифровых отпечатков (рис. 3.84).

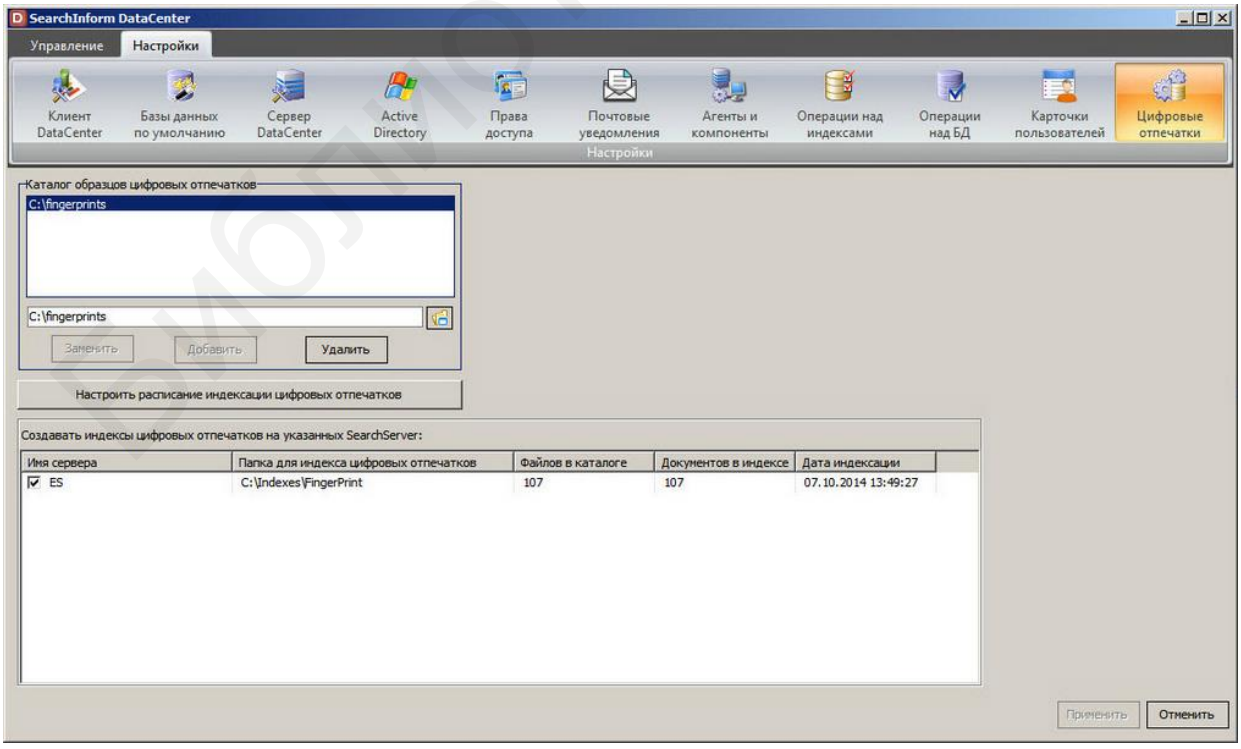


Рис. 3.84. Каталог цифровых отпечатков

Использование журналов событий. В журнале изменений (рис. 3.85) протоколируются следующие события: добавление, удаление и редактирование пользователей, критериев поиска, политик и индексов. Для просмотра журнала изменений необходимо выделить элемент «Журнал изменений».

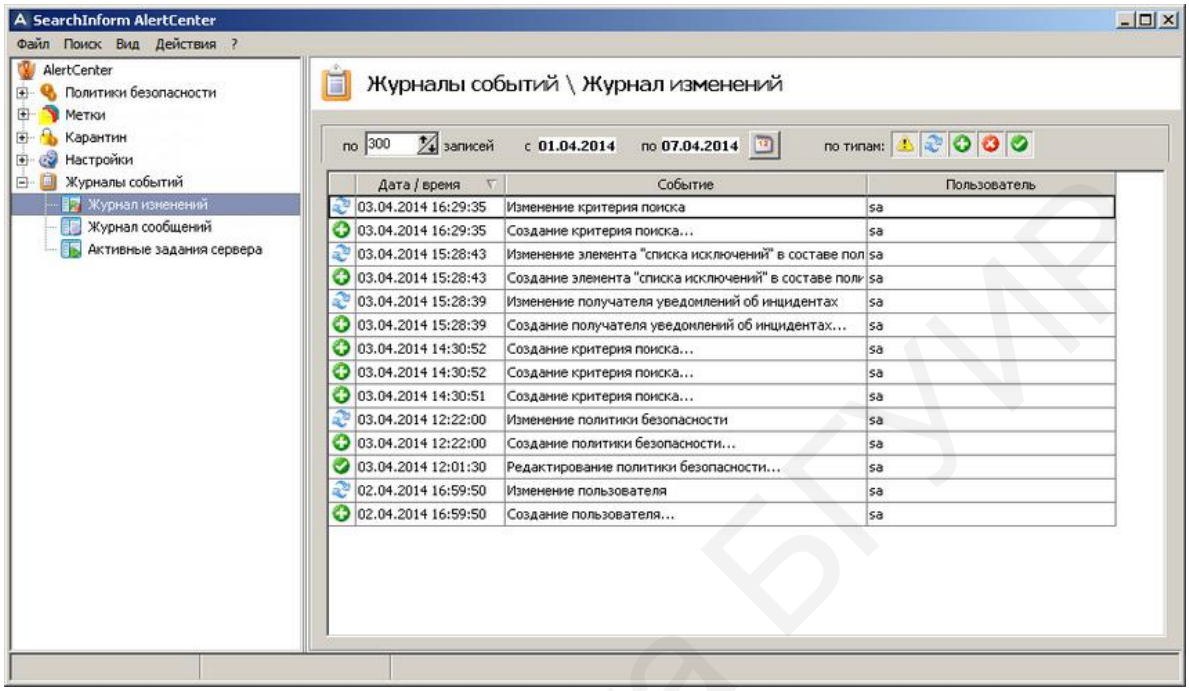


Рис. 3.85. Протоколирование событий в журнале изменений

Протокол событий можно фильтровать по числу записей, а также по типу событий. Для включения отображения событий в логе используются следующие кнопки:

– предупреждение;

– последнее изменение в критериях поиска и настройках;

– добавление критериев поиска, регулярных выражений и цифровых отпечатков;

– удаление критериев поиска, регулярных выражений и цифровых отпечатков;

– редактирование критериев поиска.

В журнале сообщений (рис. 3.86) протоколируются события, связанные с работой службы проверки: начало и завершение проверки, подключения к индексу, число найденных документов, генерация уведомлений. Для просмотра журнала сообщений следует выделить элемент «Журнал сообщений». Возможна фильтрация по числу записей и по дате.

Журнал сообщений отображает следующие события:

– начало и завершение проверок;

– подключение к серверам SoftInform Search и к индексам и отключение от них;

– генерацию почтовых уведомлений;

– отключение от серверов и индексов;

Библиотека БГУИР

– остановку задач по требованию.

Для отображения статуса сообщений используются значки:

– комментарии к действиям системы;

– уведомления системы;

– предупреждения системы;

– ошибки системы;

– команды, отданные оператором.

Для включения подсветки сообщений, относящихся к разным группам задач, необходимо установить флажок в строке «Выделять задачи цветом». Общие задания не подсвечиваются.

При помощи установки флажка в строке «Группировать по задачам» можно производить группировку записей журнала по задачам.

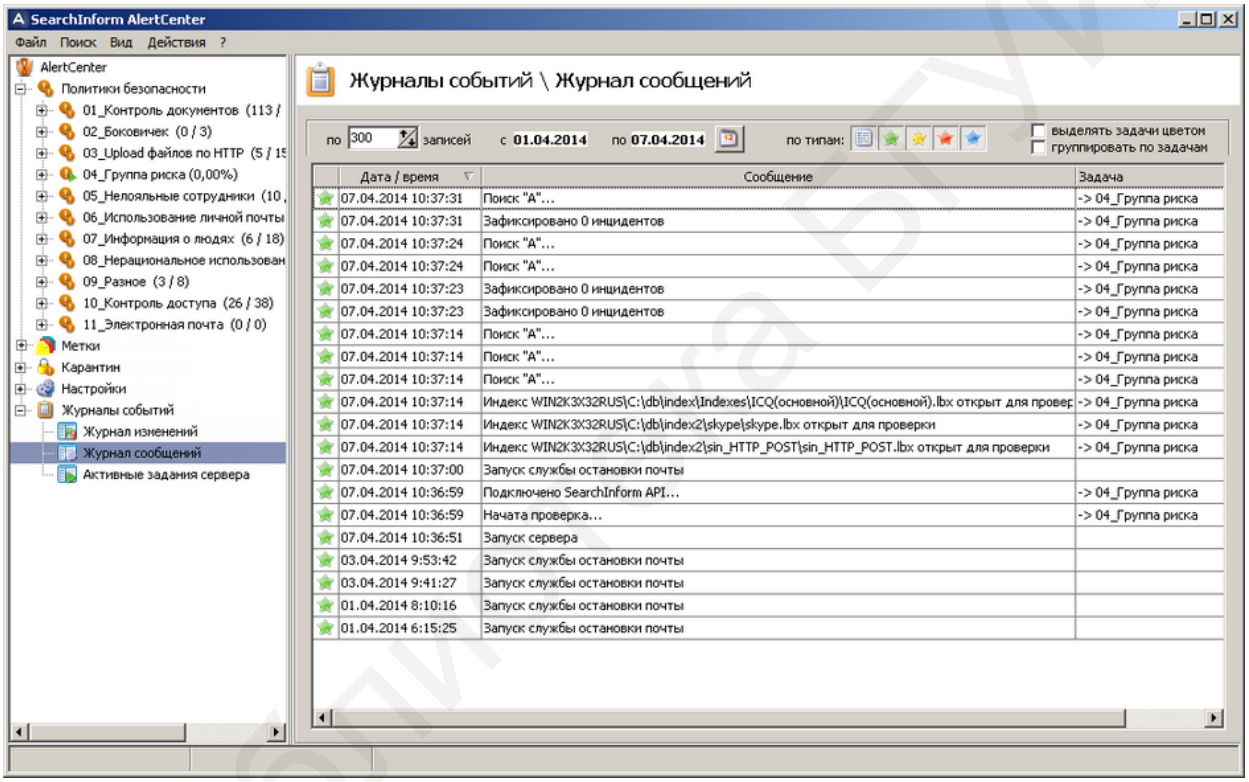


Рис. 3.86. Протоколирование событий в журнале сообщений

На вкладке «Активные задания сервера» (рис. 3.87) отображаются задачи сервера, в первую очередь, статус назначенных проверок индексов.

Для отмены задачи следует выделить ее, а затем щелкнуть правой кнопкой мыши, выбрав команду «Начать/прервать проверку».

Библиотека БГУИР

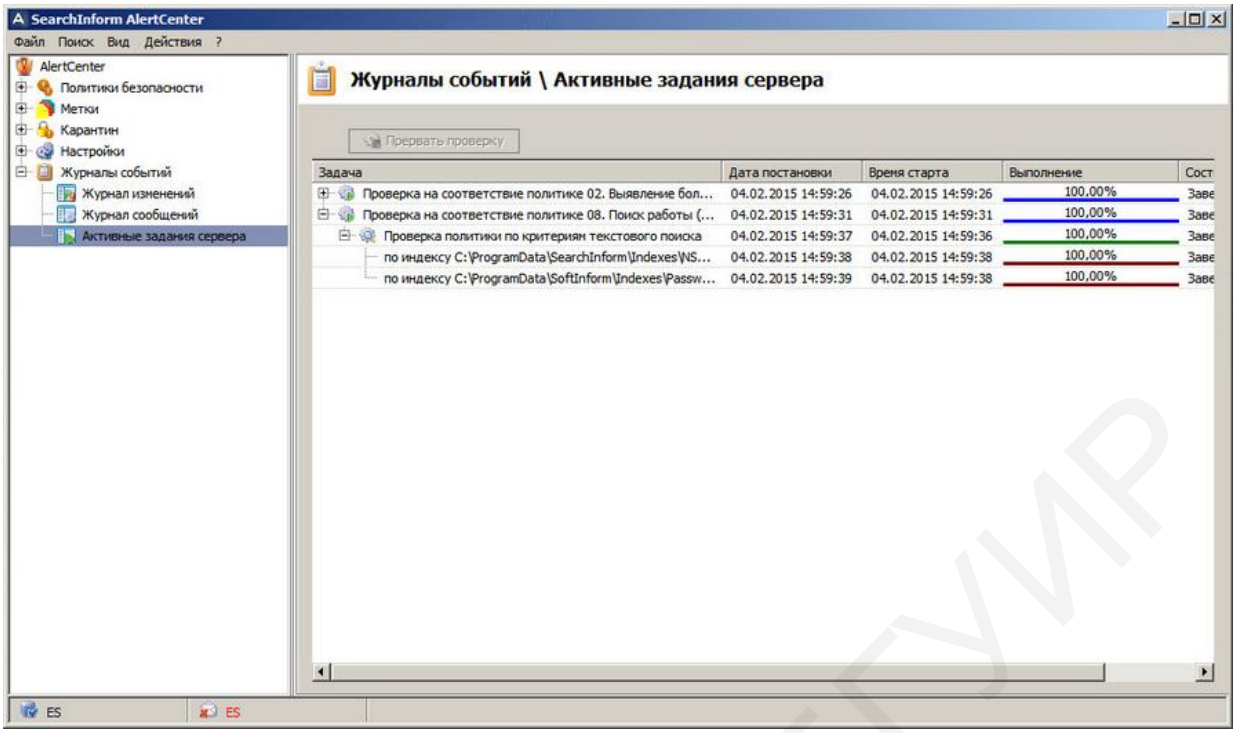


Рис. 3.87. Отображение активных заданий сервера

Все взаимодействия с сервером AlertCenter осуществляются через сервер баз данных. Поэтому возможны задержки при большом числе срабатываний сервера.

Если на вкладке «Активные задания» не отображаются время и статус текущей операции, а индикатор выполнения задач стоит на 0 % и не изменяется, необходимо проверить соединение с сервером. Наиболее вероятные причины отсутствия связи:

– сервер AlertCenter остановлен;

– сервер AlertCenter привязан к другой базе данных.

3.3. Формирование отчетов об активности пользователей и инцидентах при помощи приложения SearchInform ReportCenter

Общая характеристика приложения SearchInform ReportCenter [6]. Программный продукт SearchInform ReportCenter входит в состав КИБ и предназначен для подключения к базам и индексам компонентов системы безопасности, обработки информации по статистике инцидентов, активности пользователей и генерации отчетов в удобной для сотрудников службы безопасности форме.

Для получения необходимых данных ReportCenter подключается к базе инцидентов компонента AlertCenter, базам данных EndpointSniffer и ProgramSniffer, индексам, созданным для компонентов DeviceSniffer, FTPSniffer, HTTPSniffer, IMSniffer, MailSniffer, PrintSniffer, SkypeSniffer, LyncSniffer, ViberSniffer.

Библиотека БГУИР

Благодаря поддержке указанных компонентов Searchinform ReportCenter обеспечивает построение отчетов по следующим классам переданной пользователями информации:

– документы, записанные на USB-носители, CD/DVD-матрицы и другие накопители;

– файлы, отправленные и полученные по FTP-соединению;

– сообщения, отправленные в форумы, блоги и иные сервисы при помощи веб-форм, поддерживающих POST-метод;

– сообщения IM-клиентов (ICQ, MSN, QIP и др.);

– сообщения электронной почты, отправленные при помощи клиентов или почтовых веб-сервисов;

– документы, распечатанные на сетевых принтерах;

– сеансы текстовой и голосовой связи Skype, файлы и SMS-сообщения, переданные при помощи Skype;

– сеансы текстовой и голосовой связи Viber, файлы, переданные при помощи Viber, а также списки контактов;

– текстовые и голосовые сообщения, а также файлы, переданные посредством MS Lync;

– показатели активности пользователей в запускаемых ими приложениях.

Сгенерированные отчеты могут быть представлены как в табличной форме, так и виде диаграмм, временного графика, а также графа отношений, отображающего регулируемую визуализацию связей между пользователями, находящимися в контакте.

Принцип работы SearchInform ReportCenter (рис. 3.88). Приложение включает в себя две части, привязанные к одной базе данных под управлением Microsoft SQL Server 2005+ (база ReportCenter), – серверную и клиентскую.

Серверная часть Searchinform ReportCenter получает статистику инцидентов из баз AlertCenter, данные по установке агентов и программного обеспечения из баз EndpointSniffer и статистику перехвата из индексов DeviceSniffer, FTPSniffer, HTTPSniffer, IMSniffer, MailSniffer, PrintSniffer, SkypeSniffer, соотносит статистику со списком пользователей каталога Active Directory и записывает полученную статистику в базу данных.

Клиентская часть подключается к базе Searchinform ReportCenter, интерпретирует статистические данные и формирует отчеты в формате таблиц, диаграмм, графика, а также в виде интерактивного графа отношений.

Характеристика основных элементов интерфейса клиентской части SearchInform ReportCenter представлена в табл. 3.22.

Библиотека БГУИР

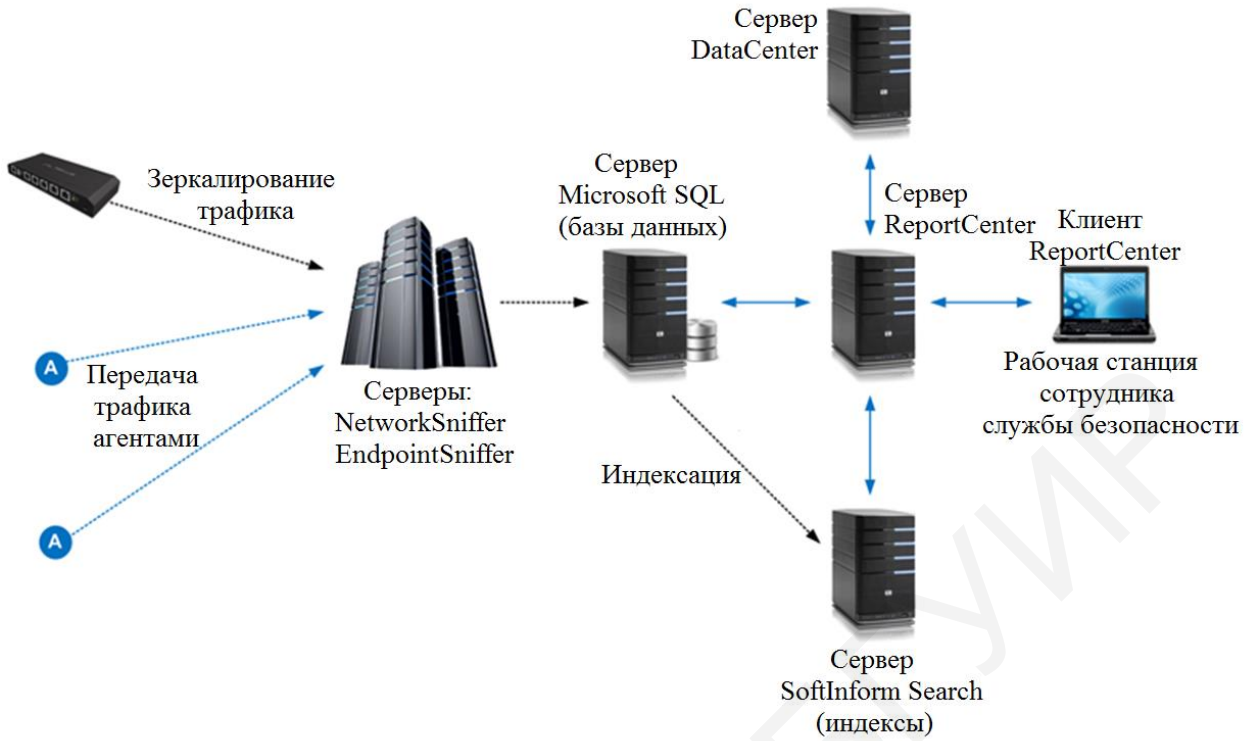


Рис. 3.88. Схема работы Searchinform ReportCenter

Таблица 3.22

Основные элементы интерфейса консоли SearchInform ReportCenter

Наименование элемента	**Назначение**
Панель выбора шаблонов отчета	Отображает список шаблонов, на основании которых генерируются отчеты. С помощью расположенных в верхней части кнопок-иконок предусмотрена возможность создания новых шаблонов отчетов, редактирования либо удаления уже существующих (если они были созданы пользователем), настройки базы данных клиентского модуля ReportCenter
Панель выбора периода и пользователей	Позволяет задать временной период отчета, количество отображаемых в отчетах пользователей и непосредственно произвести выборку пользователей
Окно просмотра отчетов	Отображается сгенерированный отчет. С помощью кнопок-иконок возможна навигация по отчетам, их детализация, экспортирование отчета в различные форматы файлов, настройки параметров страницы и вывода отчета на печать. Окно просмотра позволяет также сохранить сгенерированный отчет в виде отдельного (пользовательского) шаблона. Каждый сгенерированный отчет (диаграмма, таблица или интерактивный граф) отображается в окне просмотра в виде отдельной вкладки

Клиентская часть SearchInform ReportCenter. Подключение к базе данных ReportCenter необходимо, чтобы получать статистические данные, на основании которых в дальнейшем будут строиться отчеты. Клиент должен быть подключен к той же базе данных ReportCenter, что и сервер.

Библиотека БГУИР

При помощи сервера можно создать новую базу ReportCenter. В этом случае клиент ReportCenter также следует привязать к новой базе данных ReportCenter. Для этого необходимо воспользоваться кнопкой «Настройки базы данных» (рис. 3.89). Вызов окна настройки базы данных может быть также произведен через выбор опции «Настройки базы данных» в меню «Настройки» главного окна клиента ReportCenter.

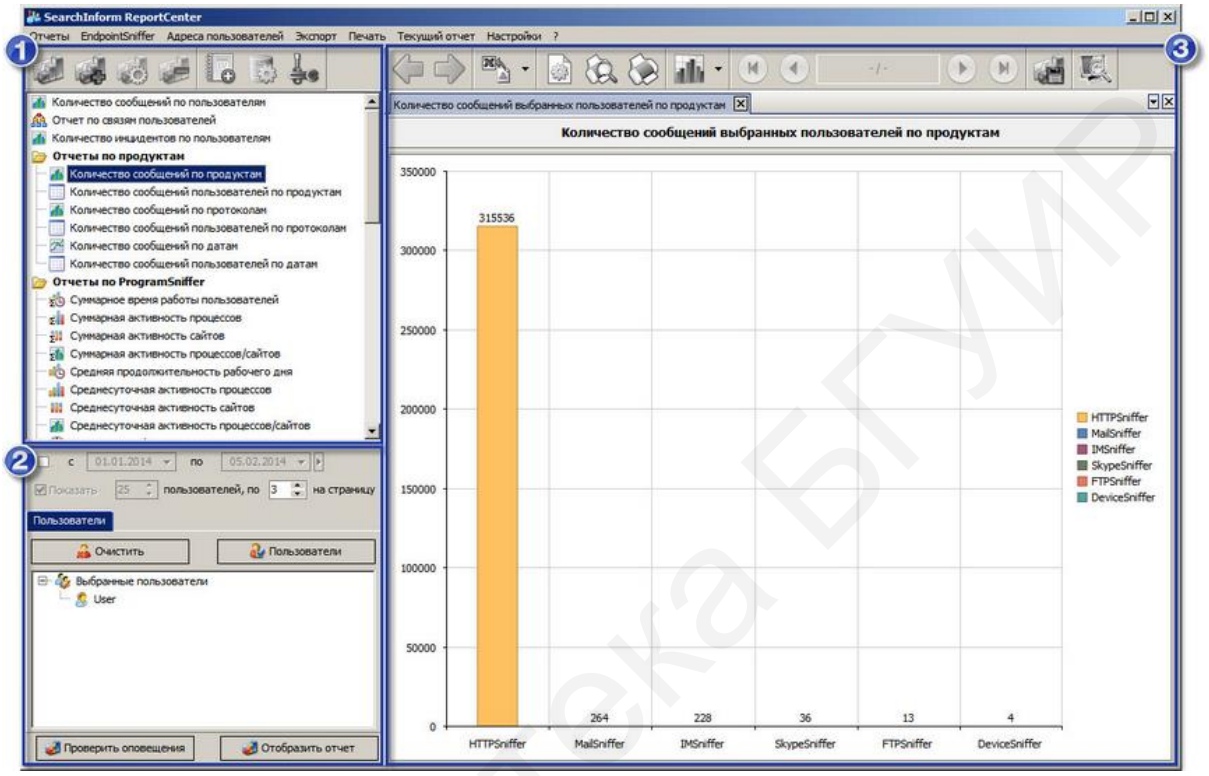


Рис. 3.89. Интерфейс клиентской части SearchInform ReportCenter

При помощи серверной консоли можно создать новую базу ReportCenter. В этом случае клиент ReportCenter также необходимо привязать к новой базе данных ReportCenter. Для этого воспользуйтесь кнопкой «Настройки базы данных». В появившемся окне выберите компьютер, на котором установлена серверная часть ReportCenter, и нажмите «ОК» (рис. 3.90). Клиент ReportCenter будет подключен к базе данных выбранного сервера ReportCenter.

ReportCenter позволяет *выбрать временной период, за который будет сгенерирован тот или иной отчет*. Выбор временного периода производится на панели выбора периода и пользователей в строке настройки временного интервала (рис. 3.91).

По умолчанию отчеты формируются за все время, при этом элементы настройки временного периода неактивны. Для указания конкретного временного периода необходимо установить соответствующий флажок.

Кнопка ▶ служит для генерации отчета за предустановленный период (за предыдущие сутки, неделю, месяц, год). Список доступных для выбора временных периодов устанавливается в настройках интерфейса. Для ввода произвольного периода времени необходимо указать начальную и конечную даты

Библиотека БГУИР

в формате (ДД-ММ-ГГГГ) или нажать кнопку для вызова календаря. Отчет за указанный временной период будет отображен в окне просмотра после нажатия кнопки «Отобразить отчет» в нижней части консоли.

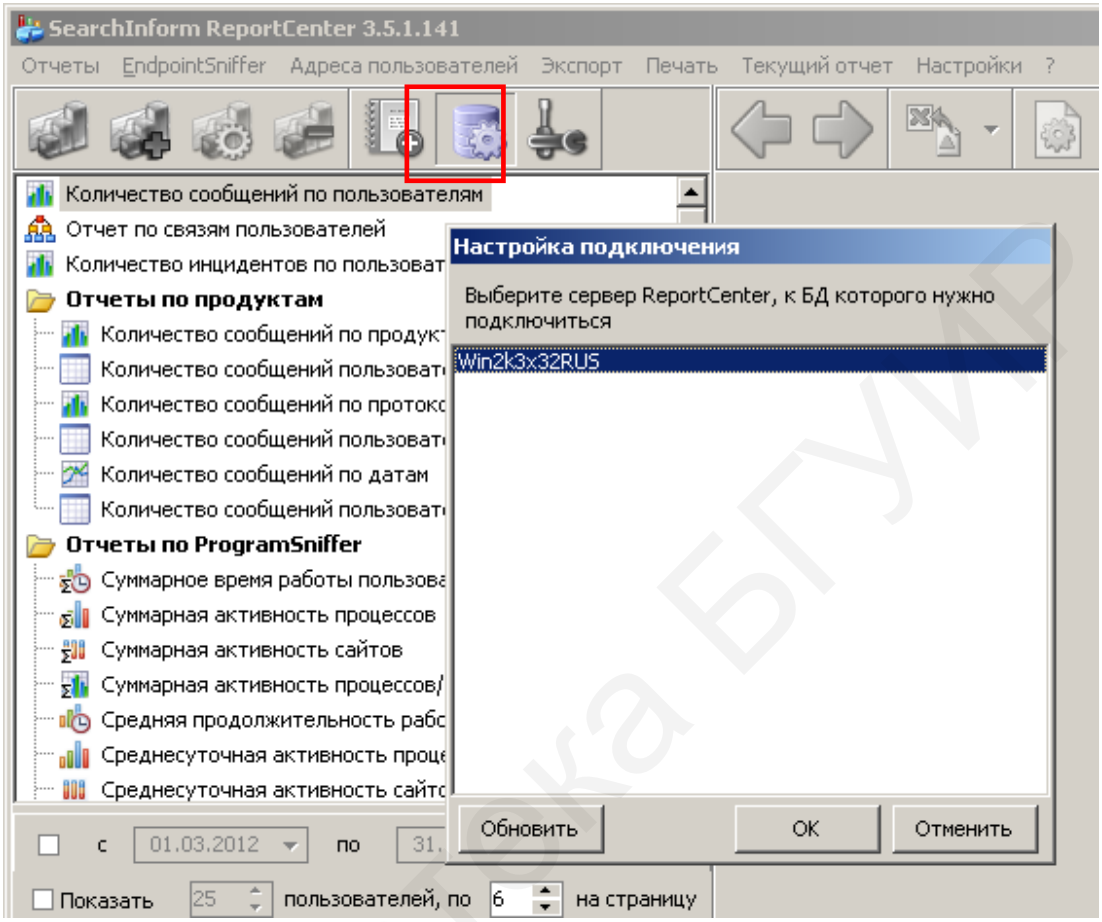


Рис. 3.90. Настройки базы данных

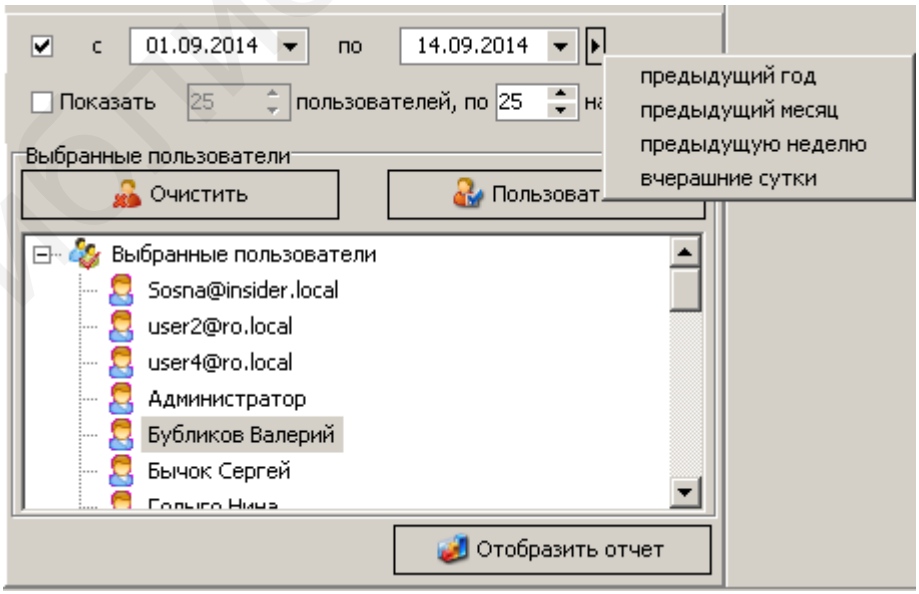


Рис. 3.91. Выбор временного периода,
за который будет сгенерирован тот или иной отчет

Библиотека БГУИР

Выбор пользователей. Отчеты можно генерировать как по всем, так и по отдельным пользователям. Выбор пользователей домена производится на панели фильтров.

Под строкой настройки временного периода расположена строка выбора количества отображаемых пользователей, позволяющая задать следующие настройки:

– количество выбранных пользователей, отображаемых в отчете;

– число пользователей, которое будет отображаться на каждой странице отчета.

По умолчанию первая настройка отключена. Это означает, что в отчете отображаются все выбранные пользователи. Для ограничения числа отражаемых в отчете пользователей следует установить соответствующий флажок (перед словом «Показать») и задать необходимое значение. После нажатия кнопки «Отобразить отчет» в графе отношений будут отображены наиболее активные выбранные пользователи (т. е. те, которые за указанный период времени имели наибольшее количество сообщений) в количестве, равном выставленному значению.

Другая настройка всегда находится в активном состоянии, позволяя указать количество отображаемых на каждой странице пользователей при представлении отчета в виде диаграммы.

Для выбора пользователей домена из списка на вкладке «Пользователи» необходимо нажать кнопку «Пользователи» (рис. 3.92).

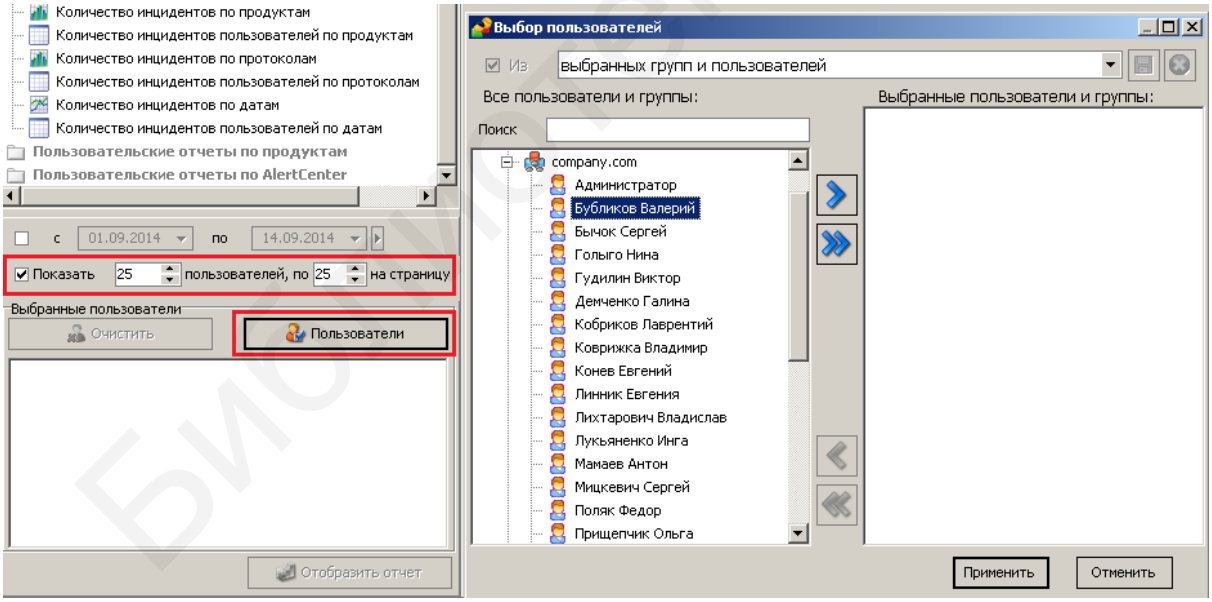


Рис. 3.92. Выбор пользователей домена для формирования отчета

В левой части открывшегося окна «Выбор пользователей» отображается список доступных пользователей, в правой части окна – список входящих в выборку пользователей. Если пользователи не выбраны, генерируется отчет по умолчанию, т. е. для всех пользователей.

Выбор пользователей производится при помощи следующих кнопок:

– для отдельных выделенных пользователей и групп;

– для пользователей и групп, входящих в состав выделенной группы.

Удаление пользователей из списка выбранных производится при помощи двух кнопок:

– для выделенных пользователей и групп;

– для всех добавленных в выборку пользователей и групп.

Также выбор и удаление пользователей можно производить по двойному щелчку кнопки мыши.

Подтверждение выбора пользователей производится с помощью кнопки «Применить».

Для быстрого поиска по списку пользователей предусмотрено текстовое поле «Поиск». По мере ввода поискового запроса или комбинации букв совпадения, найденные в полях «имя», «фамилия» или «логин», отображаются в формате <domain\user> (рис. 3.93).

Список доменов и их пользователей ReportCenter считывает из базы данных продукта DataCenter, который в свою очередь получает и обновляет данные из Active Directory. Пользователи, удаленные из Active Directory, не исчезают физически из базы данных DataCenter. Считывая таких пользователей, ReportCenter помещает их в группу «Удаленные пользователи» (рис. 3.94). По данным пользователям также можно строить отчеты (вплоть до времени их удаления).

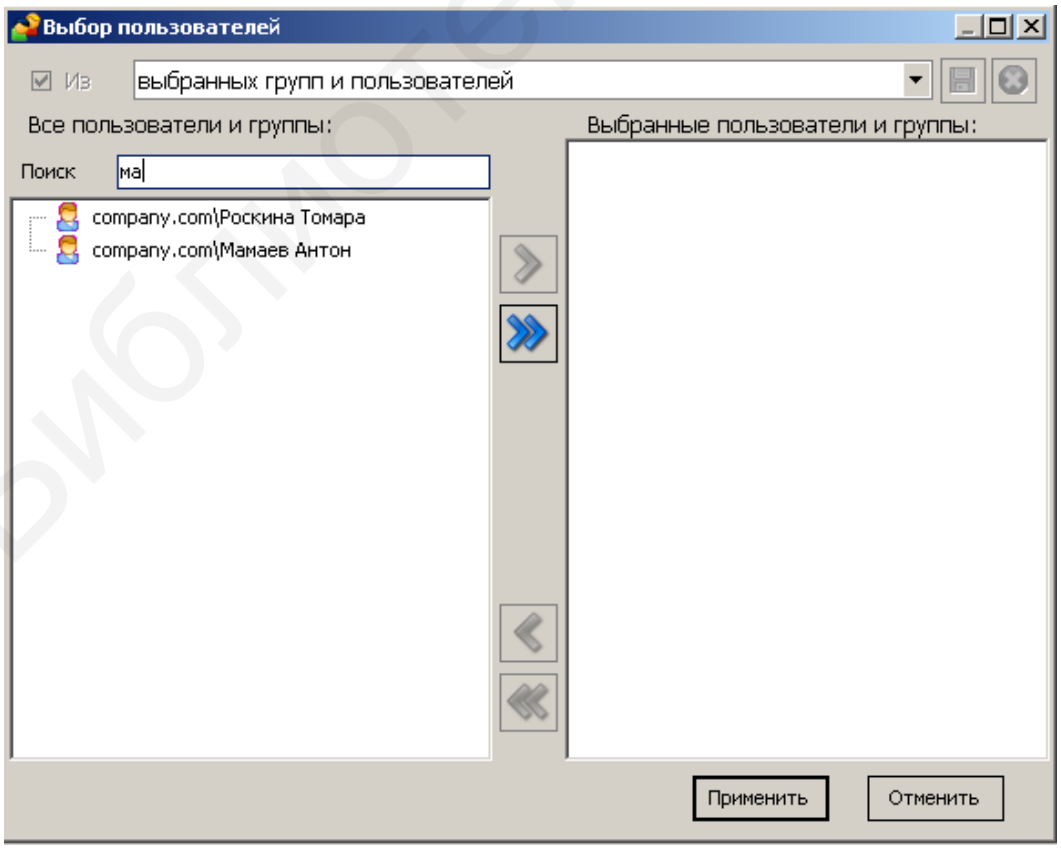


Рис. 3.93. Быстрый поиск по списку пользователей

Библиотека БГУИР

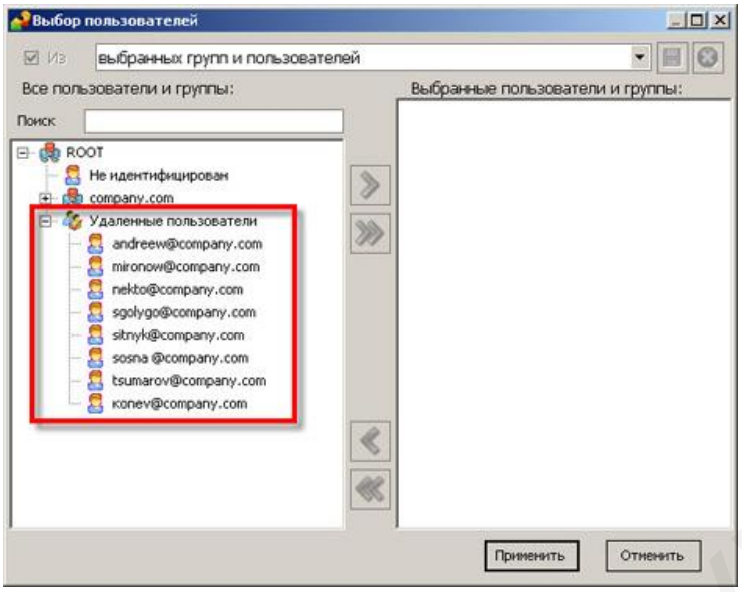


Рис. 3.94. Группа «Удаленные пользователи»

В группу «Удаленные пользователи» также помещаются пользователи, по которым имеются перехваченные данные в индексах, но сам пользователь отсутствует в Active Directory и/или в базе данных DataCenter. Как вариант можно предположить ситуацию, когда пользователь был добавлен в Active Directory, но DataCenter еще не произвел синхронизацию данных и ReportCenter в свою очередь не смог сопоставить перехваченные данные с имеющимся в базе данных именем доменного пользователя. После синхронизации с Active Directory DataCenter получит данные о новом пользователе, и тот будет перемещен из группы «Удаленные пользователи» в соответствующий домен.

Включенные в выборку пользователи в списке доступных пользователей отображаются другим цветом.

Список выбранных пользователей можно сохранить как отдельную выборку. Для этого необходимо воспользоваться кнопкой  и ввести имя выборки (рис. 3.95).

Список созданных пользователем выборок можно просмотреть с помощью выпадающего списка. Для удаления открытой выборки следует нажать кнопку  .

Полная очистка списка выбранных пользователей производится при помощи кнопки «Очистить».

Отчет по выбранным пользователям будет отображен в окне просмотра после нажатия кнопки «Отобразить отчет».

В последних версиях ReportCenter отчеты можно генерировать не только по пользователям, но также по компьютерам и программам.

Выбор программ и выбор компьютеров производится аналогично выбору пользователей.

Генерация отчетов осуществляется на панели выбора шаблонов отчетов. В базовую поставку ReportCenter входит ряд предустановленных шаблонов

Библиотека ТУСУР

отчетов, а также предусмотрена возможность добавления и настройки новых форматов отчетов.

В комплект поставки ReportCenter включены следующие группы шаблонов отчетов:

– общие отчеты;
– отчеты по продуктам;
– отчеты по ProgramSniffer;
– отчеты по AlertCenter;
– отчеты по программам;
– отчеты EndpointSniffer:
– отчеты по устройствам.

Рис. 3.95. Сохранение выбранных пользователей как отдельной выборки

Отчеты могут быть представлены в виде таблиц, диаграмм, графика, а также в виде интерактивного графа (только для отчетов по связям пользователей). Для табличных отчетов используется пиктограмма  , для диаграмм –  , для временных графиков –  , для интерактивного графа –  .

В число общих отчетов входят:

– диаграмма «Количество сообщений по пользователям»;
– граф «Отчет по связям пользователей»;
– диаграмма «Количество инцидентов по пользователям».

В число отчетов по продуктам (отчетов по статистике перехвата продуктами программного комплекса «Контур информационной безопасности SearchInform» входят:

– диаграмма «Количество сообщений по продуктам»;

– таблица «Количество сообщений пользователей по продуктам»;
– диаграмма «Количество сообщений по протоколам»;
– таблица «Количество сообщений пользователей по протоколам»;
– диаграмма «Количество сообщений по датам»;
– таблица «Количество сообщений пользователей по датам».

В число отчетов по ProgramSniffer (отчетов по активности пользователей и приложений/сайтов) входят:

– суммарное время работы пользователей;
– суммарная активность процессов;
– суммарная активность сайтов;
– суммарная активность процессов/сайтов;
– среднесуточная продолжительность рабочего дня;
– среднесуточная активность процессов;
– среднесуточная активность сайтов;
– среднесуточная активность процессов/сайтов;
– детальная информация по пользователям;
– поиск по активности пользователей;
– поиск по активности процессов/сайтов;
– отсутствовавшие пользователи;
– опоздания сотрудников;
– ранние уходы;
– журнал рабочего времени;
– нарушения рабочего режима;
– посещения сотрудников;
– табель рабочего времени.

В число отчетов по AlertCenter (отчетов по нарушениям политик информационной безопасности, обнаруженным компонентом AlertCenter) входят:

– диаграмма «Количество инцидентов по группам»;
– таблица «Количество инцидентов пользователей по группам»;
– диаграмма «Количество инцидентов по политикам»;
– таблица «Количество инцидентов пользователей по политикам»;
– диаграмма «Количество инцидентов по продуктам»;
– таблица «Количество инцидентов пользователей по продуктам»;
– диаграмма «Количество инцидентов по протоколам»;
– таблица «Количество инцидентов пользователей по протоколам»;
– диаграмма «Количество инцидентов по датам»;
– таблица «Количество инцидентов пользователей по датам».

В число отчетов по программам входят:

– количество компьютеров по программам;
– количество установок программ;
– количество удалений программ;
– компьютеры с неустановленными программами;
– программы, установленные на компьютерах;
– изменение программ на компьютерах.

Библиотека БГУИР

В число отчетов по устройствам входят:

– изменения устройств на компьютерах;

– устройства на компьютерах.

В число отчетов по EndpointSniffer входят:

– установленное ПО;

– история установки ПО;

– история установки агентов;

– количество сообщений по компьютерам.

Для отображения отчета в консоли клиентского приложения ReportCenter следует выбрать тип отчета, например, «Количество сообщений по продуктам»; если требуется, указать временной интервал, по которому будет производиться запрос; после чего добавить пользователей, по данным которых будет сгенерирован отчет, и нажать кнопку «Отобразить отчет» (рис. 3.96).

При этом если лицу, работающему с ReportCenter, был запрещен из консоли DataCenter просмотр данных по кому-либо из выбранных пользователей, то отчеты по таким пользователям отображаться не будут.

В общем случае в окне просмотра отчетов могут производиться следующие операции:

– детализация отчетов;

– просмотр контекстно связанных отчетов;

– перемещение по отчетам;

– экспорт отчета (с возможностью выбора формата);

– настройка страницы;

– предварительный просмотр отчета;

– печать отчета;

– переключение между режимами отображения;

– вывод отчетов по целесообразности использования сотрудниками рабочего времени;

– представление отчетов по связям пользователей в виде графа отношений;

– перемещение по многостраничным отчетам;

– сохранение отчета в виде пользовательского шаблона;

– вызов внешнего приложения.

Сгенерированный отчет, будь то диаграмма, таблица, график или интерактивный граф, отображается в окне просмотра в виде отдельной вкладки. Для навигации по открытым вкладкам предназначены как навигационные стрелки, так и выпадающий список открытых вкладок, который открывается при помощи нажатия стрелки .

Для закрытия выбранной вкладки используется кнопка .

Библиотека БГУИР

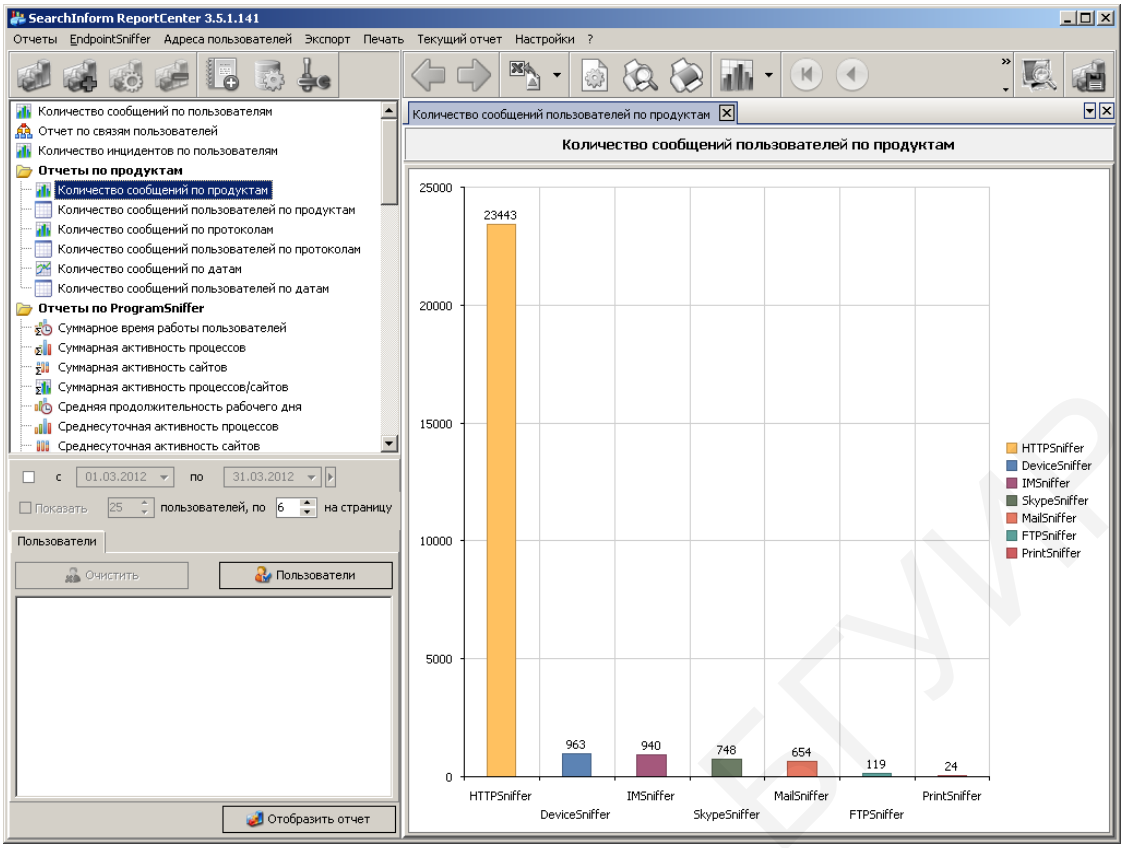


Рис. 3.96. Отображение отчета «Количество сообщений по продуктам»

Детализация отчетов. Под детализацией отчетов понимается возможность переходов на частные отчеты при помощи щелчка правой или левой кнопкой мыши по соответствующему столбцу диаграммы, заголовку колонки или строке таблицы. При этом в настройках клиента должна быть включена опция «Разрешить автопереходы». Существуют следующие варианты детализации:

– по пользователям: статистика по всем пользователям / по группам пользователей домена / по отдельным пользователям домена;

– по времени: статистика за все время / по годам / по месяцам / по дням (дополнительно можно включить детализацию по кварталам);

– по инцидентам: все инциденты / инциденты по политикам безопасности / инциденты по отдельным критериям;

– по продуктам: все перехваченные документы / документы по продуктам / документы по протоколам;

– по рабочему времени: статистика за все время / по годам / по месяцам / по дням.

Рассмотрим пример детализации. При генерации отчета активности пользователей будет отображено число документов, перехваченных продуктами (MailSniffer, IMSniffer...). При щелчке кнопкой мыши по столбцу MailSniffer будет отображено число документов, перехваченных по отдельным протоколам (SMTP, HTTP, POP3 и др.). При щелчке по столбцуSMTP будет отображено число документов, перехваченных за все время, затем последовательно по годам, месяцам, дням.

Библиотека БГУИР

Просмотр контекстно связанных отчетов. При щелчке правой кнопкой мыши по столбцу диаграммы, заголовку строки и столбцу таблицы может открываться контекстное меню со списком связанных отчетов. Например, если открыта общая статистика перехвата по продуктам, а в контекстном меню продукта MailSniffer выбрана команда «Инцидентов по протоколам», будет открыта статистика инцидентов по поддерживаемым почтовым протоколам.

Перемещение по отчетам, открытым в соседних вкладках, производится с помощью стрелок навигации  и  . Перемещение по отчетам выполняется аналогично переходам по веб-страницам.

Отчеты можно экспортировать в файлы форматов XLS, HTML, TXT, XML, PDF. Для экспорта отчета в файл используется кнопка  .

Вызов окна параметров страницы осуществляется при помощи кнопки  . Доступны следующие настройки страницы: размер бумаги, ориентация, последовательность печати листов, размеры полей, вид колонтитулов и масштаб по отношению к оригиналу.

Вызов окна предварительного просмотра отчета осуществляется при помощи кнопки  .

Печать отчета осуществляется при помощи кнопки  .

Для смены режима представления отчета используется выпадающий список. В окне просмотра отчетов может производиться переключение между, например, табличным и диаграммным режимами отображения. Табличные отчеты отображают не только количество документов или сообщений, но также и их объем (рис. 3.97).

Перемещение по многостраничным отчетам. Большие отчеты могут не уместиться на одну страницу. В таком случае переход по страницам осуществляется при помощи кнопок:

 – на первую страницу отчета;

 – на предыдущую страницу отчета;

 – на следующую страницу отчета;

 – на последнюю страницу отчета.

В случае когда базовых шаблонов отчетов недостаточно, можно добавить свой шаблон. Любой сгенерированный отчет может быть сохранен как отдельный (пользовательский) шаблон. Для этого необходимо воспользоваться кнопкой «Создать шаблон отчета» (рис. 3.98).

Библиотека БГУИР

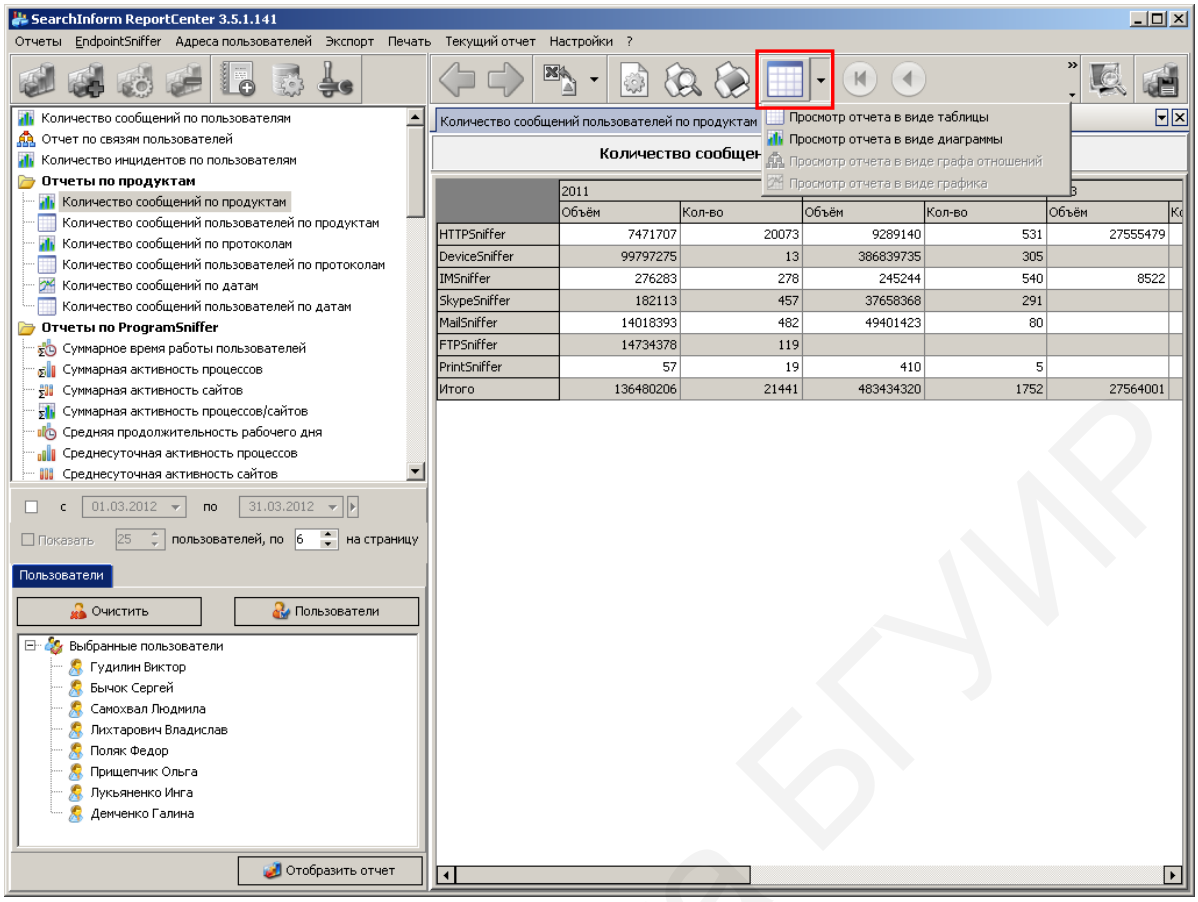


Рис. 3.97. Отображение отчета «Количество сообщений по продуктам» в виде таблицы

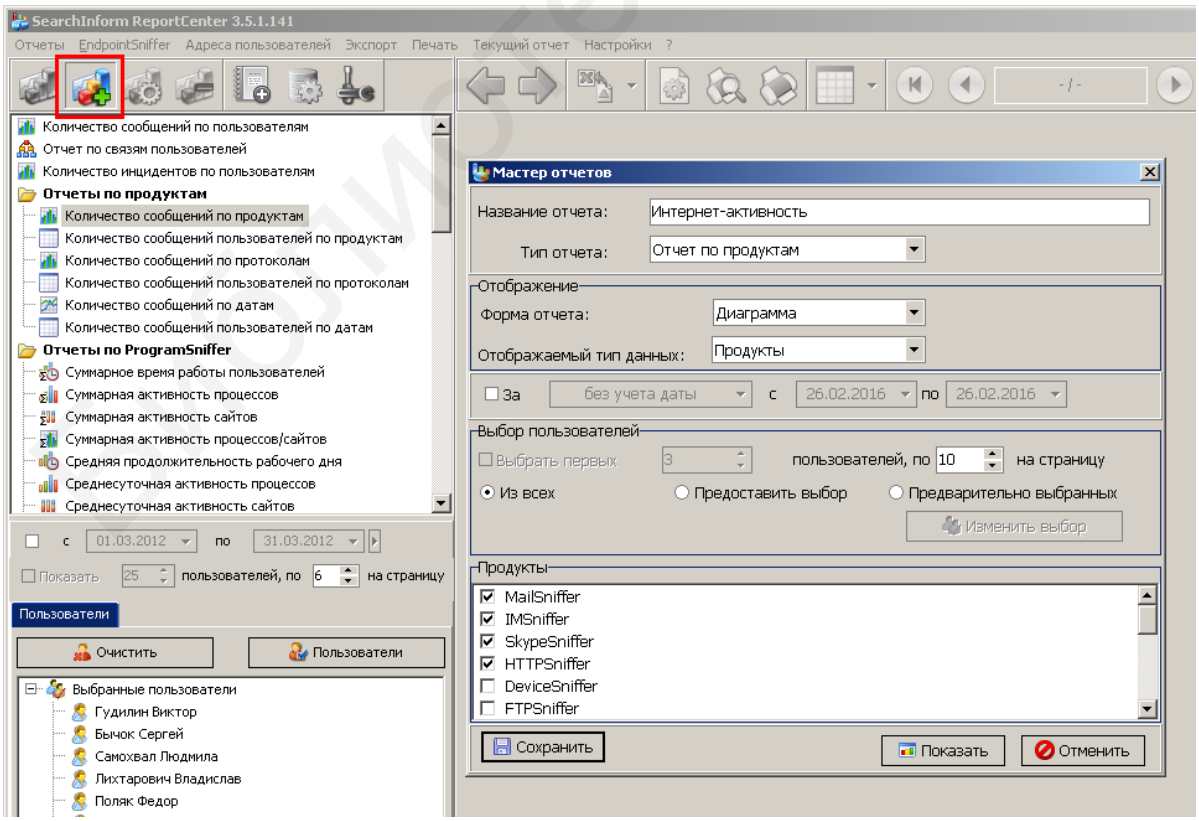


Рис. 3.98. Создание шаблона отчета

В появившемся окне необходимо ввести название добавляемого отчета, выбрать его форму (диаграмма или таблица) и тип (отчет по продуктам или отчет по инцидентам AlertCenter). В случае необходимости следует настроить временной интервал, произвести выбор пользователей, по документам или инцидентам которых будет сформирован отчет. Также необходимо выбрать нужные продукты, установив соответствующий флажок. При формировании отчета по инцидентам также можно делать привязку к группам алертов и отдельным запросам. Для сохранения формата следует нажать кнопку «Сохранить», а для просмотра отчета без сохранения шаблона – кнопку «Показать».

Оповещения по пользователям / Оповещения по программам. Для создания пользовательского шаблона отчета ProgramSniffer в выпадающем списке «Тип отчета» выберите «Оповещения по пользователям» / «Оповещения по программам». Укажите критерии оповещения и нажмите кнопку «Сохранить» (рис. 3.99).

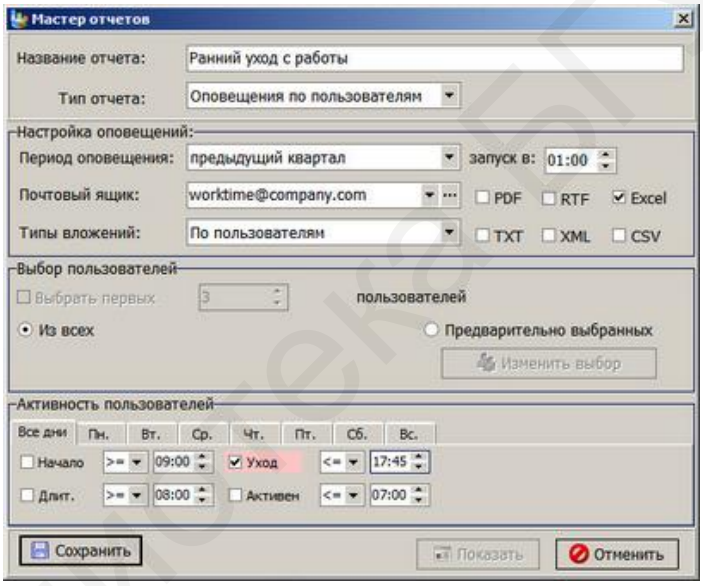


Рис. 3.99. Создание оповещения по пользователям

Созданный в данном примере отчет по сотрудникам будет сохранен в группе «Оповещения по пользователям».

При просмотре отчета в правой части консоли отображаются данные созданного отчета, а ниже – оповещения по таким событиям, как высокая активность сотрудника, длинный рабочий день, опоздания и поздний уход с работы (при этом возможен выбор варианта отображения оповещений: по пользователям, по категориям или в виде таблицы) (рис. 3.100).

Библиотека ГГТУ им.

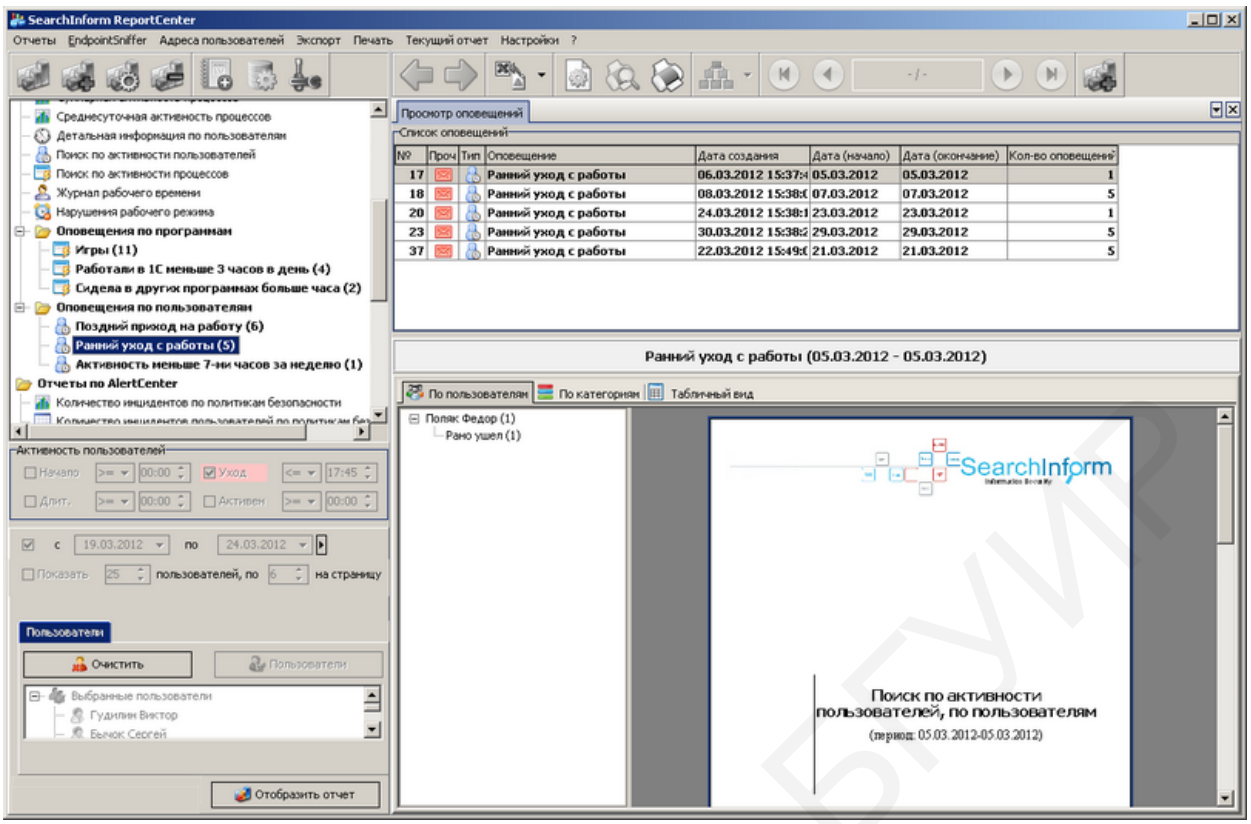


Рис. 3.100. Просмотр оповещения

Редактирование пользовательского шаблона. Созданные шаблоны отчетов можно настраивать. Для редактирования собственного шаблона необходимо выделить его и нажать кнопку «Редактировать шаблон отчета» либо воспользоваться одноименной командой контекстного меню (рис. 3.101). К примеру, для рассмотренного ранее отчета по продуктам можно изменить следующие параметры:

– имя;

– форму – диаграмма или таблица;

– тип – статистический отчет по перехваченным документам или отчет по инцидентам AlertCenter;

– отображаемый тип данных – группы пользователей и пользователи, продукты и протоколы, группы политик и политики, интервал времени;

– выбор дат;

– выбор числа пользователей;

– выбор продуктов и протоколов.

Для сохранения шаблона предназначена кнопка «Сохранить», для просмотра шаблона без сохранения – кнопка «Показать», для отмены внесенных изменений формата – кнопка «Отменить».

Библиотека БГУИР

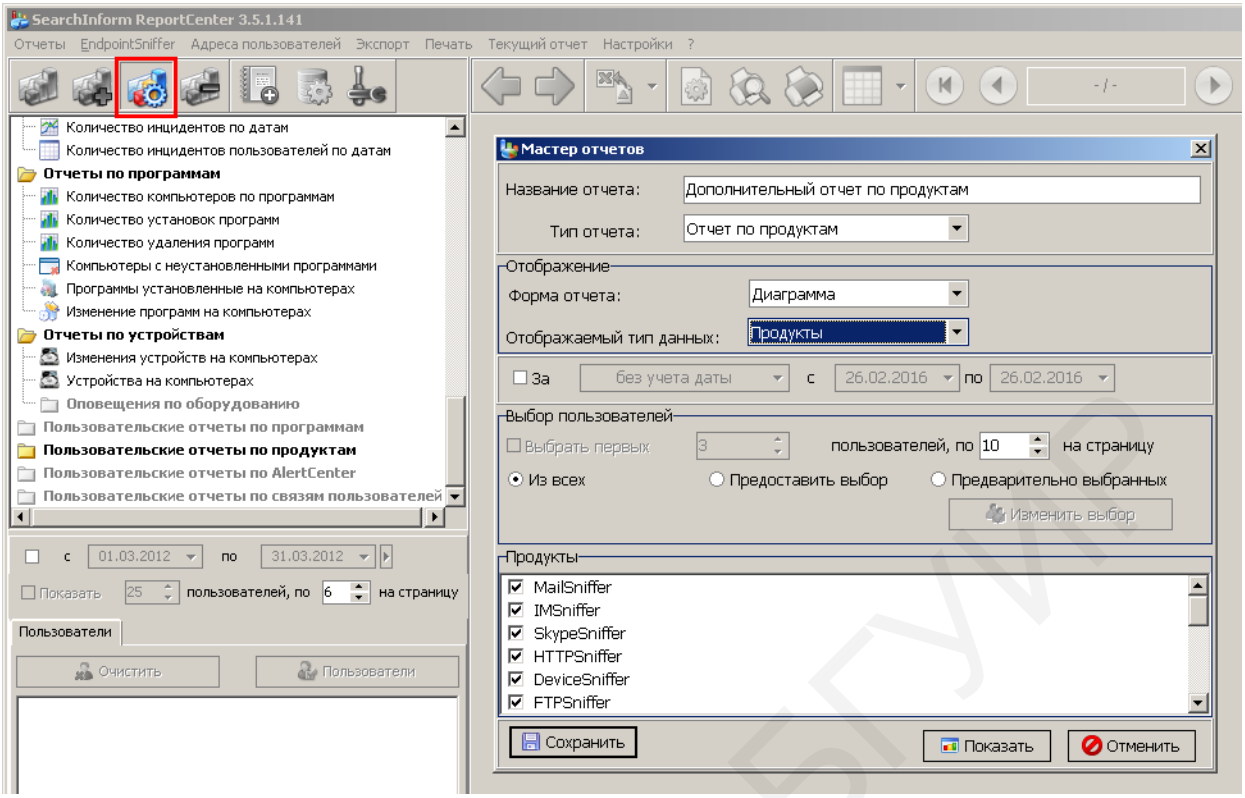


Рис. 3.101. Редактирование шаблона отчета

Выбор отображаемых шаблонов. ReportCenter позволяет определить, какие шаблоны будут отображаться в главном окне клиента, а какие – нет. Для этого следует нажать кнопку «Настройки программы» (также можно воспользоваться одноименным пунктом меню «Настройки»), в открывшемся окне настроек перейти на вкладку «Настройка списка отчетов» (рис. 3.102).

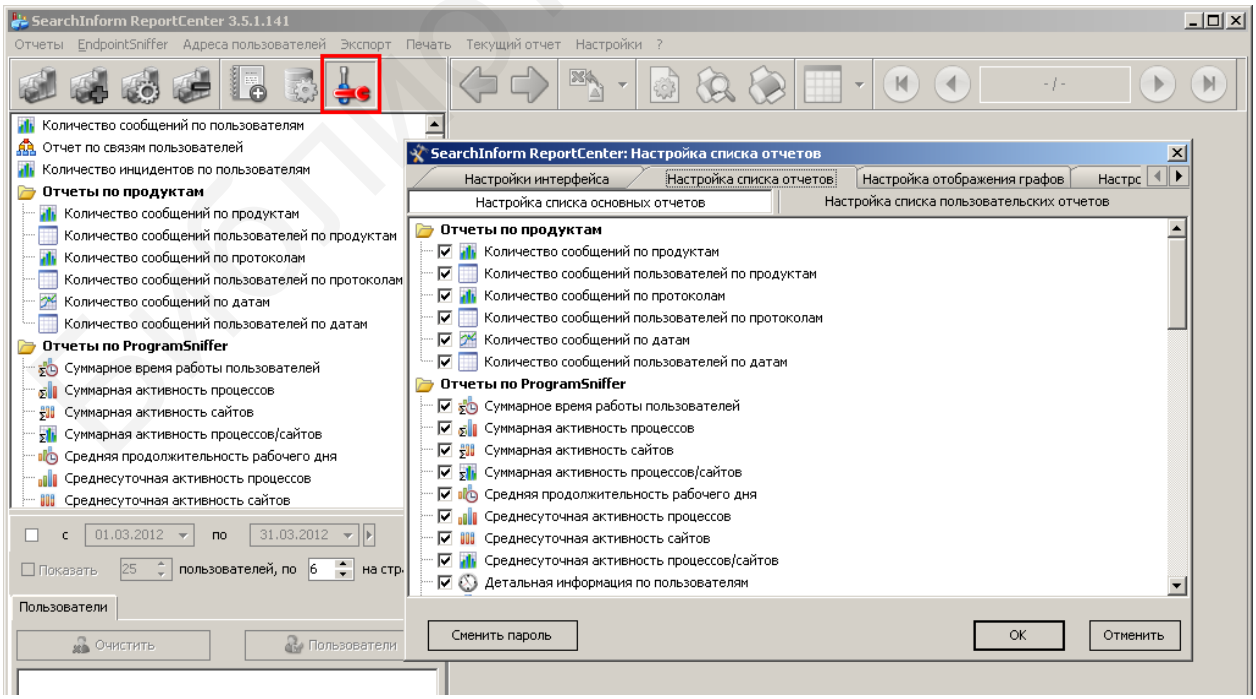


Рис. 3.102. Выбор отображаемых шаблонов

Для работы со списком основных шаблонов используется внутренняя вкладка «Настройка списка основных отчетов». Выбор производится установкой флажка перед пиктограммой типа шаблона. Для работы со списком пользовательских шаблонов предназначена внутренняя вкладка «Настройка списка пользовательских отчетов». Также можно использовать контекстное меню для скрытия/отображения отдельного отчета.

Для включения отображения всех скрытых отчетов применяется команда «Отображать скрытые отчеты» из контекстного меню, для отключения отображения – «Не отображать скрытые отчеты».

Вызов внешнего приложения. ReportCenter интегрирован с клиентскими приложениями остальных компонентов КИБ. Для работы данной функции клиентский модуль поддерживаемых компонентов должен быть установлен на один компьютер с клиентом ReportCenter. Если отображен отчет по инцидентам, указанные инциденты можно открыть в клиенте AlertCenter при помощи кнопки  . Если в отчете отображены сведения по перехвату информации продуктами, перехваченные документы можно открыть в клиентском приложении SearchInform Client при помощи кнопки  или команды «Открыть в SearchInform клиент» из контекстного меню (рис. 3.103).

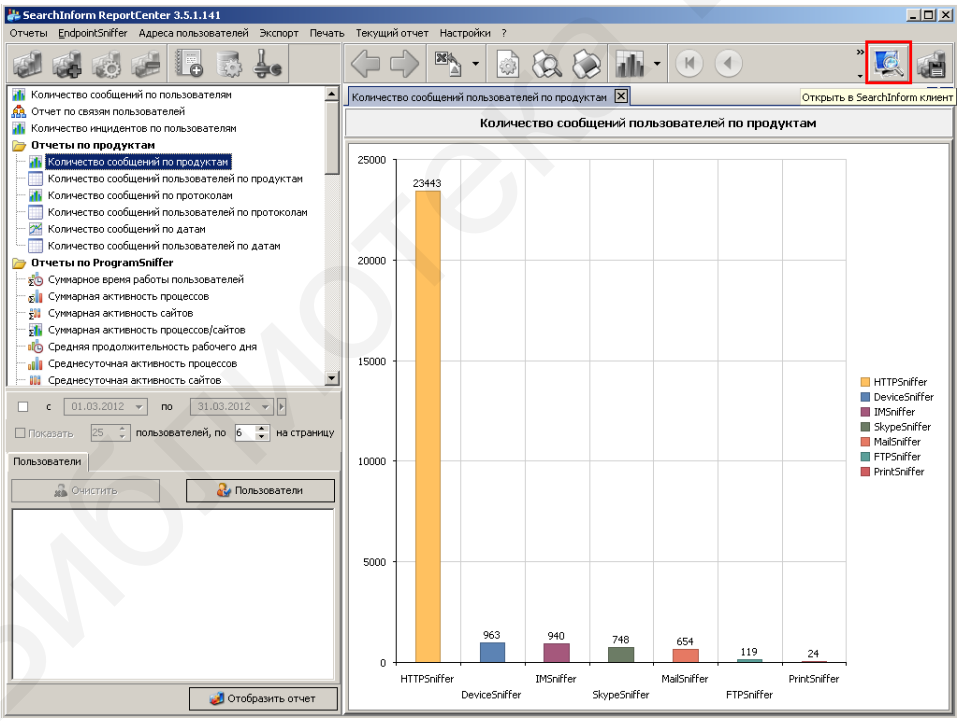


Рис. 3.103. Вызов приложения SearchInform Client

Граф отношений. Отчет в виде графа отношений позволяет выявить общих адресатов для нескольких сотрудников компании, а также проверить, использовался ли вызывающий подозрения адрес в контактах одного сотрудника другими работниками компании. Эти возможности существенно облегчают проведение служебных расследований, связанных с утечкой конфиденциальных данных и выявлением инсайдеров в организации.

Библиотека БГУИР

Для отображения графа отношений необходимо выбрать шаблон «Отчет по связям пользователей» и, соответственно, интересующих пользователей, затем настроить временной интервал, параметры отображения и нажать кнопку «Отобразить отчет» (рис. 3.104).

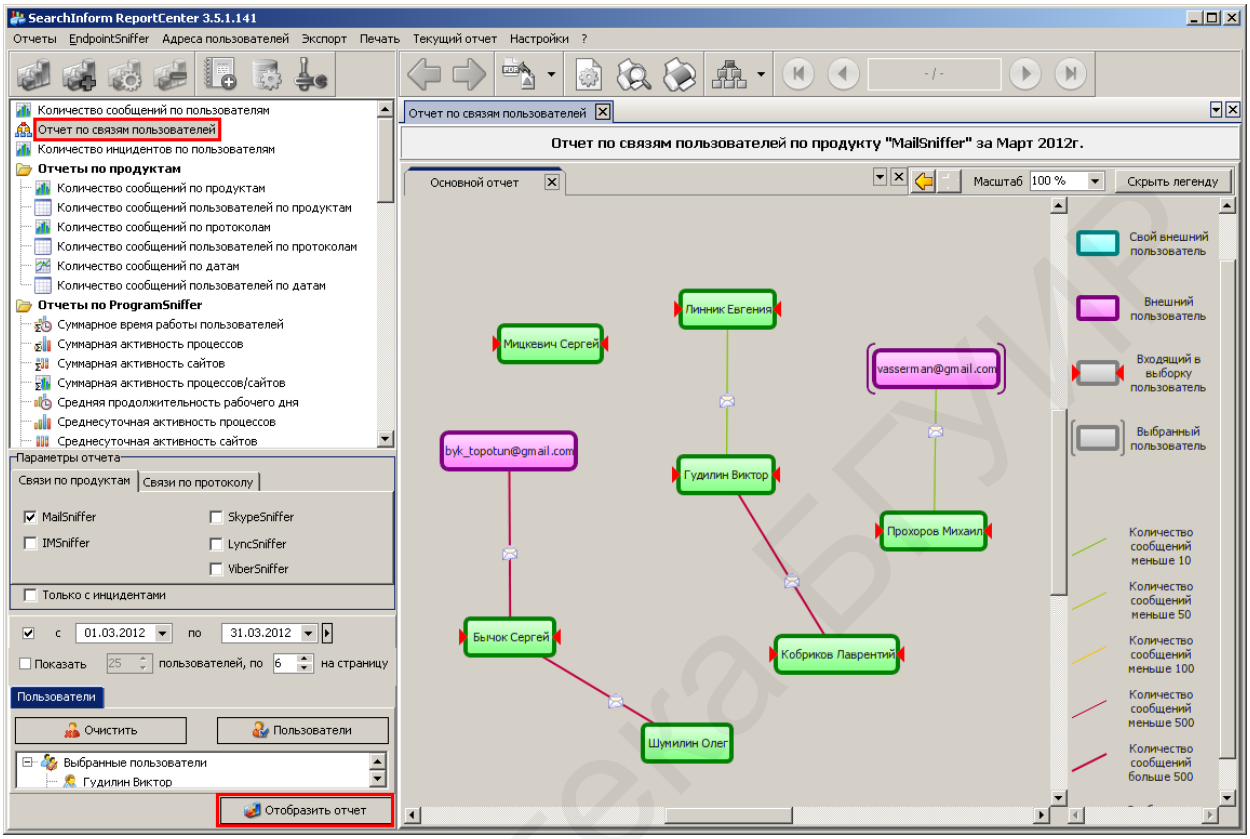


Рис. 3.104. Отображение отчета по связям пользователей

Узлы графа обозначают пользователей и их адресатов, а связывающие их ребра отображают связи. Толщина и цвет ребра зависит от количества переданных пользователями сообщений. На середине ребра отображается значок канала связи, по которому пользователь вступал в контакт с адресатом. Наведение указателя мыши на значок канала связи вызывает всплывающую подсказку с указанием пользователей, между которыми установлена связь, названия канала связи и количества сообщений, переданных по данному каналу связи. Треугольные стрелки по сторонам узла обозначают входящего в выборку пользователя. Нажатие и удержание клавиши SHIFT подсвечивает связи выделенного пользователя. Отсутствие ребра между узлами означает, что пользователи не имели контактов друг с другом в течение заданного временного периода.

Для отображения всех связей пользователя следует дважды щелкнуть кнопкой мыши по имени пользователя или, вызвав контекстное меню, выбрать команду «Развернуть» (для отображения в отдельной вкладке – «Развернуть в отдельной вкладке») (рис. 3.105).

Библиотека БГУИР

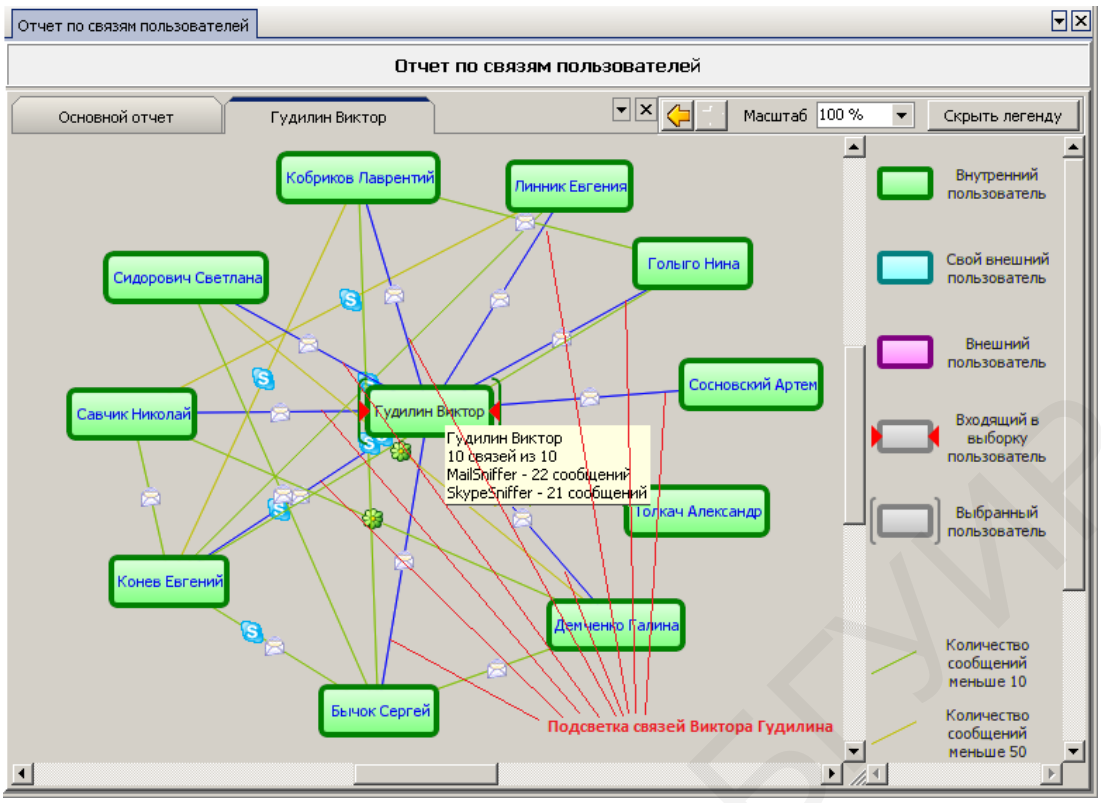


Рис. 3.105. Отображение всех связей выбранного пользователя на отдельной вкладке

Отображаемые на интерактивном графе пользователи подразделяются на три категории в зависимости от их нахождения в зоне действия системы информационной безопасности (различаются по фоновой окраске узла):

– «внутренние» – пользователи внутри системы (на рабочих станциях которых установлены компоненты системы безопасности);

– «свои внешние» – пользователи, находящиеся вне системы, но принадлежащие к данной компании (для электронной почты определяются по почтовому домену);

– «внешние» – пользователи, не принадлежащие к данной компании.

Принадлежность к той или иной категории обозначается с помощью фоновой окраски узла, которая может быть задана оператором клиента ReportCenter в окне настройки отображения графов.

Для категории внутренних пользователей в качестве имени узла выступает учетная запись пользователя (данные получаются из Active Directory), для остальных адресатов в качестве имени узла выступает адрес электронной почты, идентификатор скайпа или сервиса мгновенных сообщений, на который принимались либо с которого отправлялись сообщения.

Выделение нескольких узлов осуществляется путем последовательных щелчков кнопкой мыши по ним при удержании клавиши CTRL либо через выделение области их расположения указателем мыши.

Данный вид отчета дает возможность выявить общих адресатов для нескольких пользователей (рис. 3.106), установить, кто из сотрудников компа-

нии имел контакты с тем или иным адресатом, отследить связи пользователя с адресатами, у которых не наблюдалось общения ни с кем из других сотрудников.

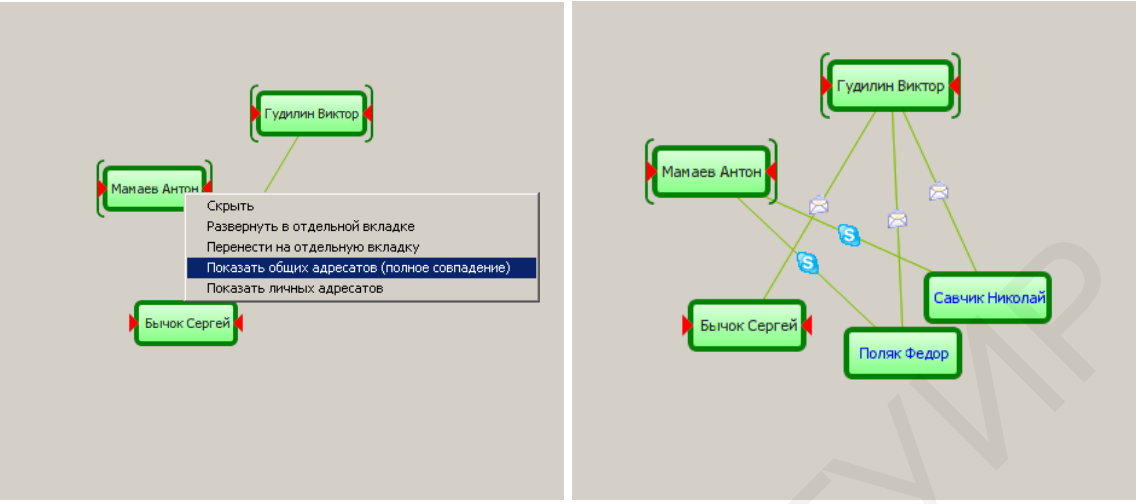


Рис. 3.106. Выявление общих адресатов для нескольких пользователей

Граф отношений может быть использован для решения следующих задач:
– отображение связей между пользователями;
– определение круга общения выбранного пользователя(-ей);
– отображение личных адресатов;
– отображение контактов внешнего пользователя с сотрудниками;
– отображение адресов пользователя;
– отображение пользователей адреса;
– выявление общих адресатов для нескольких пользователей;
– присвоение имени неизвестному адресату.

В качестве примера рассмотрим решение задачи получения с помощью графа отношений данных о контактах внешнего пользователя с внутренними (сотрудниками компании).

В окне просмотра на графе, отображающем круг общения выбранных для просмотра пользователей, выделим внешнего пользователя, контакты которого необходимо отобразить. Из контекстного меню выберем команду «Сообщений пользователей по адресату» (рис. 3.107).

В открывшемся окне отчета в виде диаграммы отобразятся внутренние пользователи, с которыми имел контакты выбранный внешний пользователь. В отличие от других отчетов, при отображении результатов в данной диаграмме будут отменены все ранее действующие фильтры (по времени, сотрудникам, каналам коммуникации). Будут отображены все внутренние сотрудники компании в зоне действия системы, состоявшие в контакте, за весь период времени, по которому хранятся данные, и по всем продуктам.

Также на диаграмме по каждому сотруднику будет указано количество сообщений, которые были отправлены выбранному внешнему адресату внутренними сотрудниками либо получены от него. Внутренние пользователи будут отображаться в порядке убывания количества полученных/отправленных

Библиотека БГУИР

сообщений. С помощью графа отношений можно присвоить неизвестному адресату имя, которое ранее было установлено (например, в ходе служебного расследования). Для этого необходимо выделить адресата и воспользоваться командой «Сопоставить адрес» из контекстного меню (рис. 3.108). В открывшемся окне соответствующий адрес следует отнести к одной из категорий («Внешние», «Свои внешние», «Внутренние»), после чего сопоставить его с именем из списка ранее проименованных адресатов либо ввести его новое имя в текстовой строке. После нажатия кнопки «Создать» выбранный адресат на графе отношений будет отображаться под новым именем. Оно будет использоваться во всех последующих сессиях работы с ReportCenter.

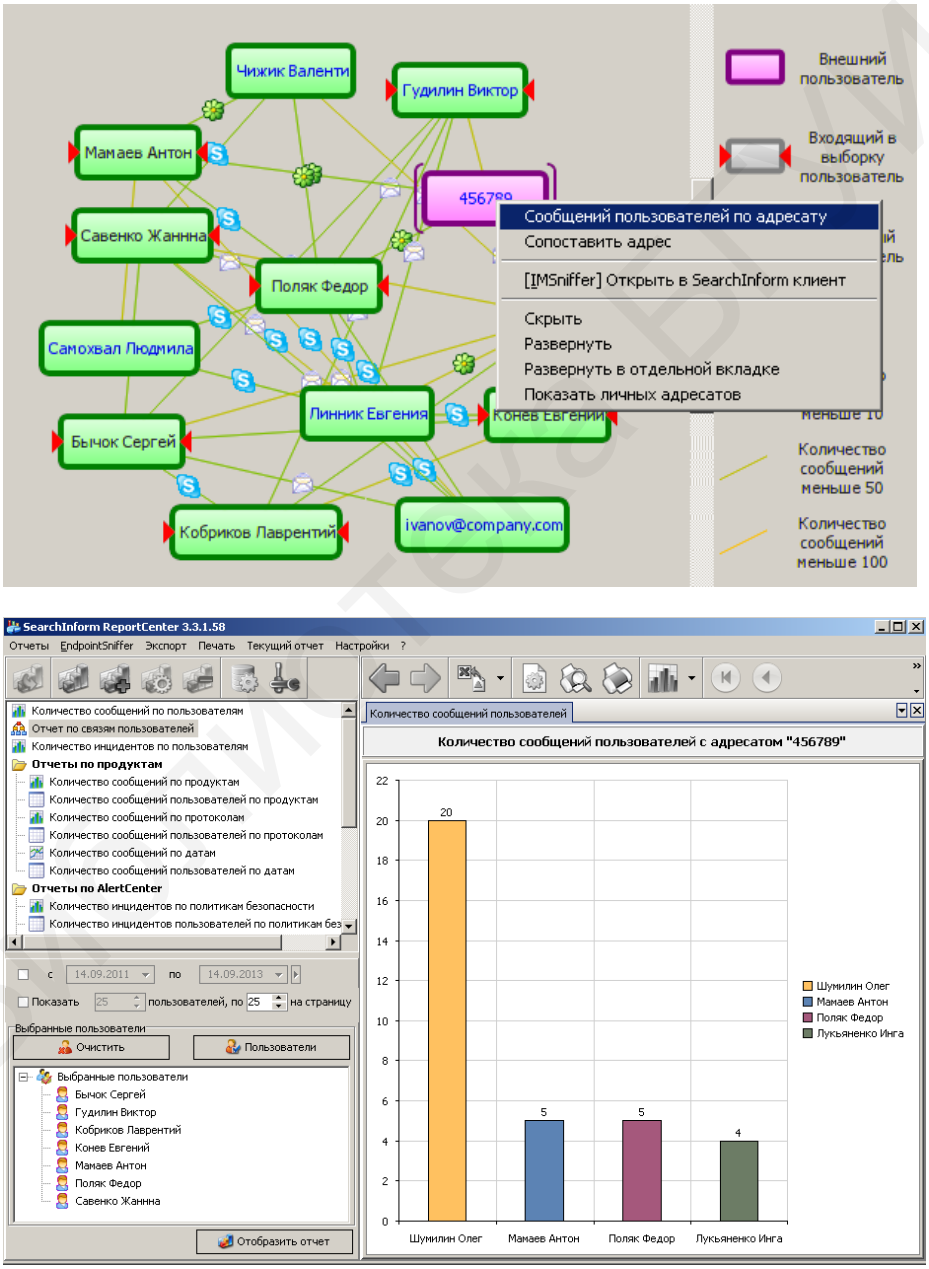


Рис. 3.107. Получение данных о контактах внешнего пользователя с работниками компании

Библиотека ВГУИР

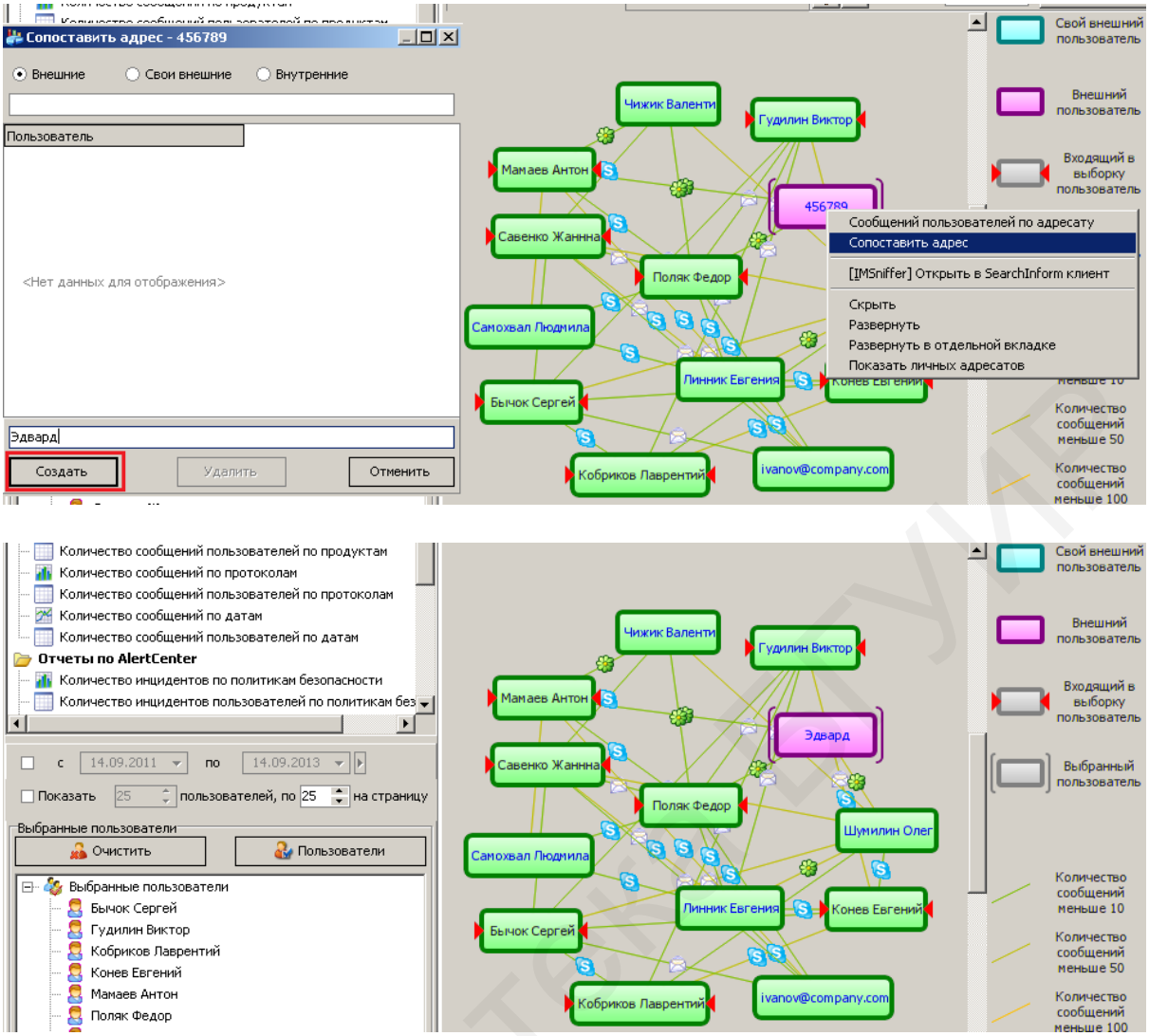


Рис. 3.108. Присвоение имени неизвестному адресату

Отчеты EndpointSniffer. Подключение к базе данных компонента EndpointSniffer позволяет выводить следующие отчеты:

– отчет по установленному на рабочих станциях программному обеспечению;

– отчет, отражающий историю установки и удаления программного обеспечения на рабочих станциях;

– отчет, представляющий собой хронологию событий, связанных с агентами: их установку, обновление и удаление.

Также предусмотрен отчет по количеству сообщений, отправленных с удаленных рабочих станций, для каждого продукта.

К каждому из отчетов можно применить функции фильтрации результатов, группировки по любому из столбцов, а также экспорт отчета во внешний файл формата *.xls.

Установленное программное обеспечение. Для просмотра перечня установленного на компьютерах программного обеспечения необходимо выбрать команду «Установленное ПО» в меню «EndpointSniffer» главного окна клиента (рис. 3.109). Отчет будет отображен в новом окне. Направление сорти-

Библиотека ГГТУ им.

ровки результатов (по возрастанию или убыванию) изменяется щелчком кнопки мыши по названию столбца.

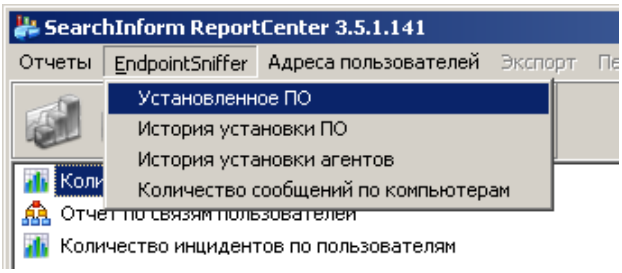


Рис. 3.109. Выбор отчетов EndpointSniffer

По умолчанию в отчете представлены сведения по всем компьютерам (рис. 3.110). Для сужения результатов выдачи, например, когда интересуют данные определенных рабочих станций, воспользуйтесь кнопкой «Выбрать компьютеры». Также можно сгруппировать результаты по любому из доступных столбцов. Для этого следует выделить заголовок столбца, по которому будет производиться группировка, и перетащить его на панель серого цвета. Одновременно можно группировать результаты поиска по нескольким условиям. Количество отображаемых колонок при этом уменьшается. Для удаления условий группировки и возврата к обычному виду просмотра необходимо перетащить параметры обратно в область отображения результатов.

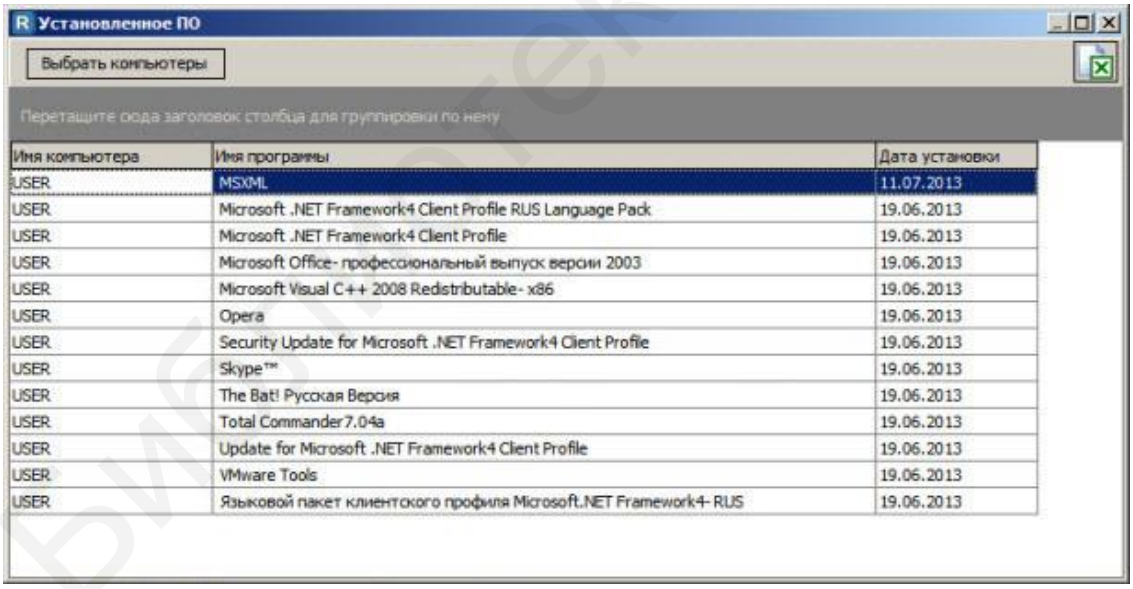
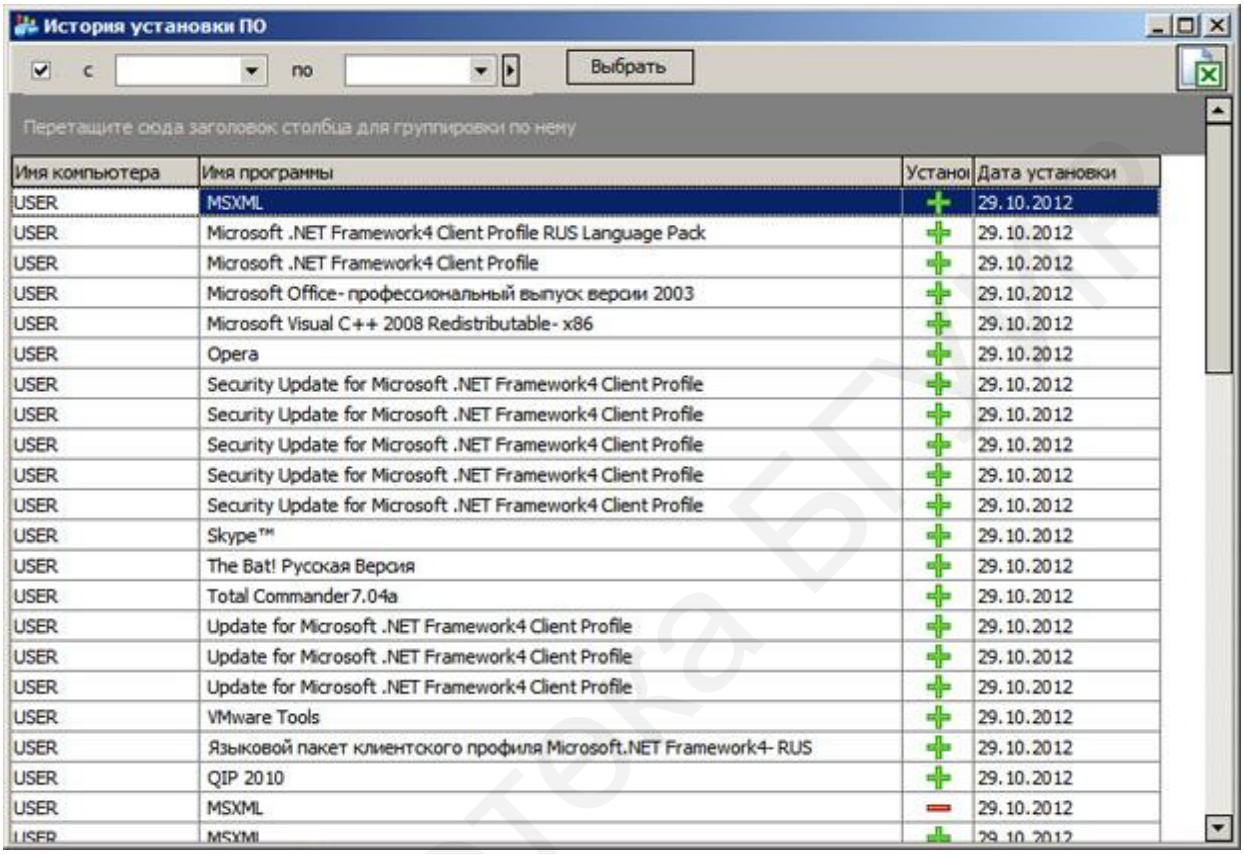


Рис. 3.110. Отчет по установленному на рабочих станциях программному обеспечению

История установки (рис. 3.111). Для просмотра истории установки и удаления на компьютерах программного обеспечения необходимо выбрать команду «История установки» в меню «EndpointSniffer» главного окна клиента. Для выборки данных только интересующего временного диапазона следует установить начальную и конечную даты с помощью календаря или воспользоваться

направляющей стрелкой для выбора одной из шаблонных заготовок: результаты за год/месяц/неделю/сутки. Сужение результатов выдачи до отдельных компьютеров, группировка по столбцам осуществляются так же, как и аналогичные действия, которые были описаны на с. 256. Для обновления списка результатов следует нажать кнопку «Отобразить отчет».



Имя компьютера	Имя программы	Установ	Дата установки
USER	MSXML	+	29.10.2012
USER	Microsoft .NET Framework4 Client Profile RUS Language Pack	+	29.10.2012
USER	Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Microsoft Office- профессиональный выпуск версии 2003	+	29.10.2012
USER	Microsoft Visual C++ 2008 Redistributable - x86	+	29.10.2012
USER	Opera	+	29.10.2012
USER	Security Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Security Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Security Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Security Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Security Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Skype™	+	29.10.2012
USER	The Bat! Русская Версия	+	29.10.2012
USER	Total Commander 7.04a	+	29.10.2012
USER	Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	Update for Microsoft .NET Framework4 Client Profile	+	29.10.2012
USER	VMware Tools	+	29.10.2012
USER	Языковой пакет клиентского профиля Microsoft.NET Framework4- RUS	+	29.10.2012
USER	QIP 2010	+	29.10.2012
USER	MSXML	−	29.10.2012
USER	MSXML	+	29.10.2012

Рис. 3.111. Отчет, отражающий историю установки
и удаления программного обеспечения на рабочих станциях

История установки агентов (рис. 3.112). Для просмотра истории установки, удаления и обновления агентов на удаленных рабочих станциях необходимо выбрать команду «История установки» в меню «EndpointSniffer» главного окна клиента. Чтобы отфильтровать операции, произведенные определенным администратором, следует установить флажок в строке «Имя администратора» и выбрать в выпадающем списке требуемое имя пользователя. Выборка данных только интересующего временного диапазона, сужение результатов выдачи до отдельных компьютеров, группировка по столбцам осуществляются так же, как и аналогичные действия, которые были описаны на с. 256.

Количество сообщений по компьютерам (рис. 3.113). Для просмотра количества сообщений, отправленных компьютерами, по каждому продукту необходимо выбрать команду «Количество сообщений по компьютерам» в меню «EndpointSniffer» главного окна клиента. Правила фильтрации результатов аналогичны рассмотренным применительно к другим отчетам.

Библиотека БГУИР

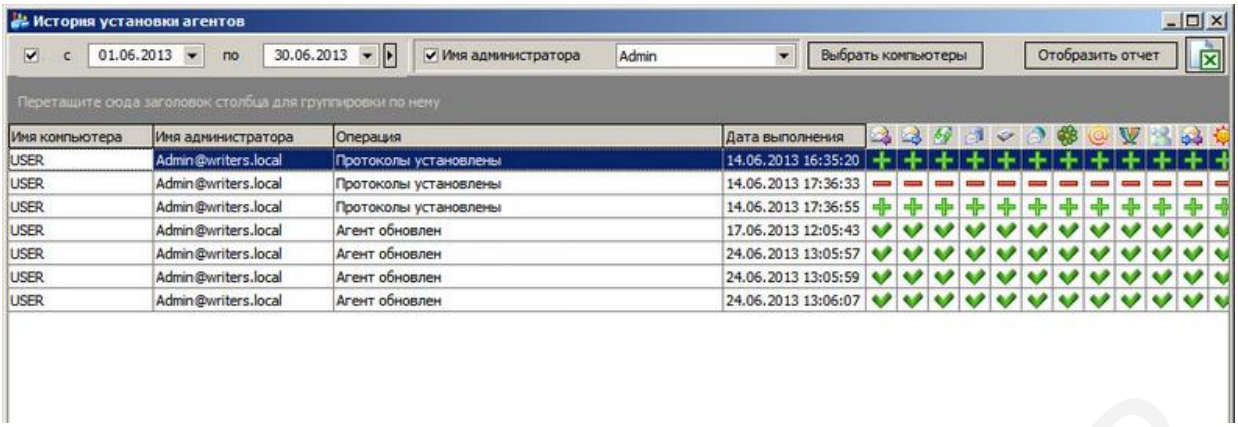


Рис. 3.112. Отчет, представляющий собой хронологию событий, связанных с агентами: их установку, обновление и удаление

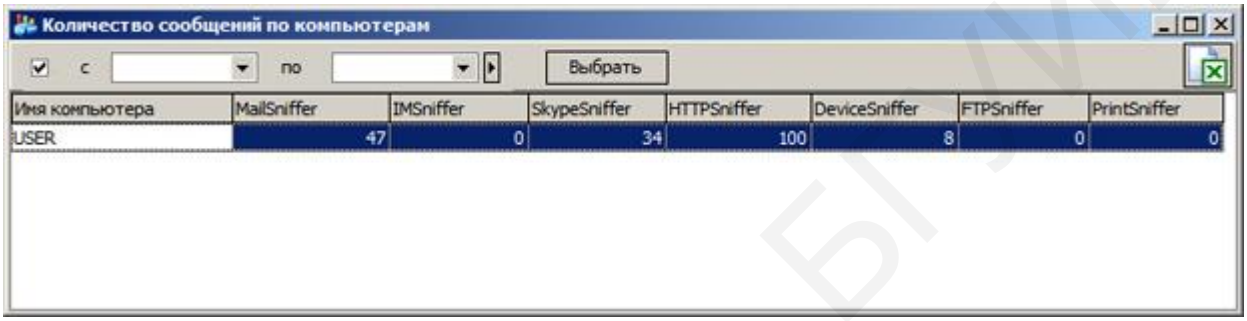


Рис. 3.113. Отчет по количеству сообщений, отправленных с удаленных рабочих станций, для каждого продукта

В группе *«Отчеты по программам»* отображаются отчеты, связанные с программным обеспечением, установленным на рабочих станциях. Отчет «Количество компьютеров по программам» показывает число компьютеров с установленными заданными программами (рис. 3.114).

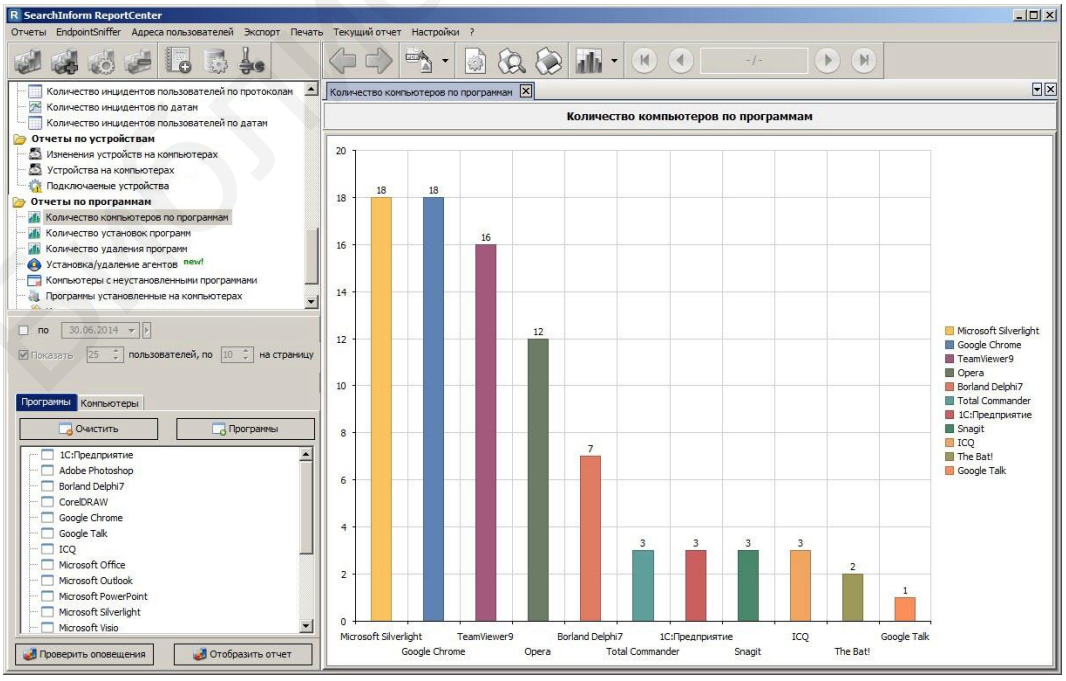


Рис. 3.114. Отчет «Количество компьютеров по программам»

Отчет «Количество установок программ» отображает число инсталляций выбранных программ на заданных компьютерах (рис. 3.115), отчет «Количество удалений программ» – число деинсталляций указанных программ на выбранных компьютерах (рис. 3.116).

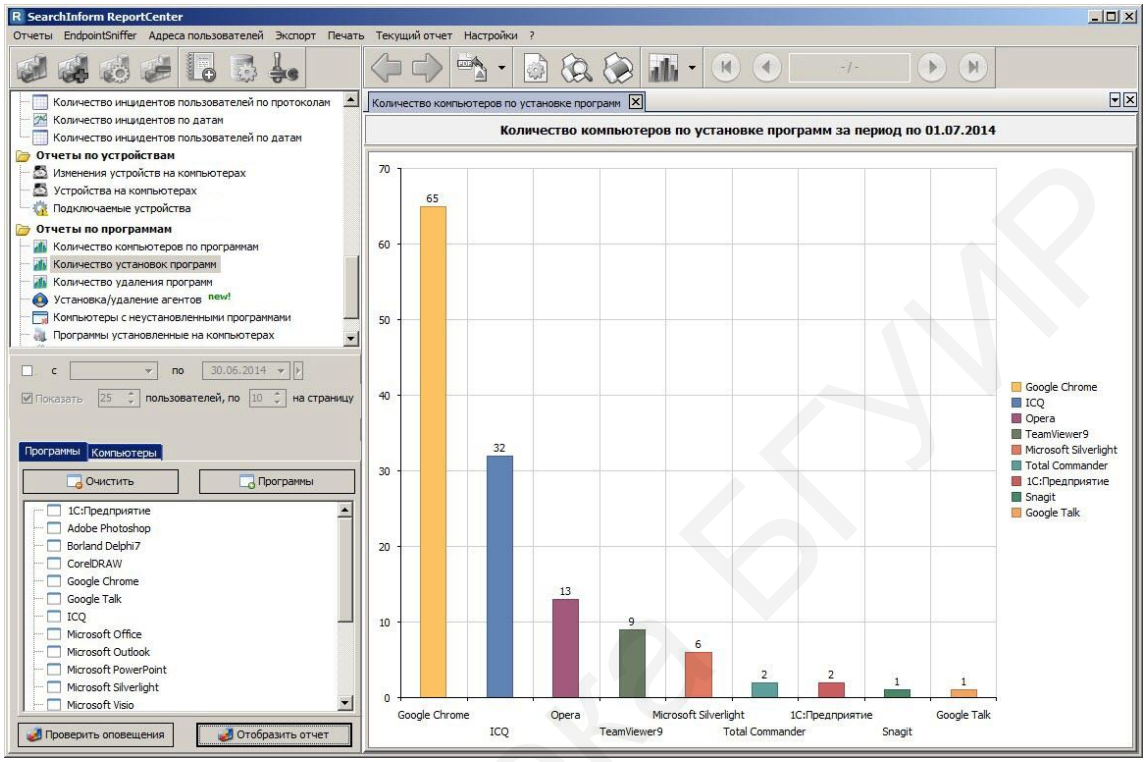


Рис. 3.115. Отчет «Количество установок программ»

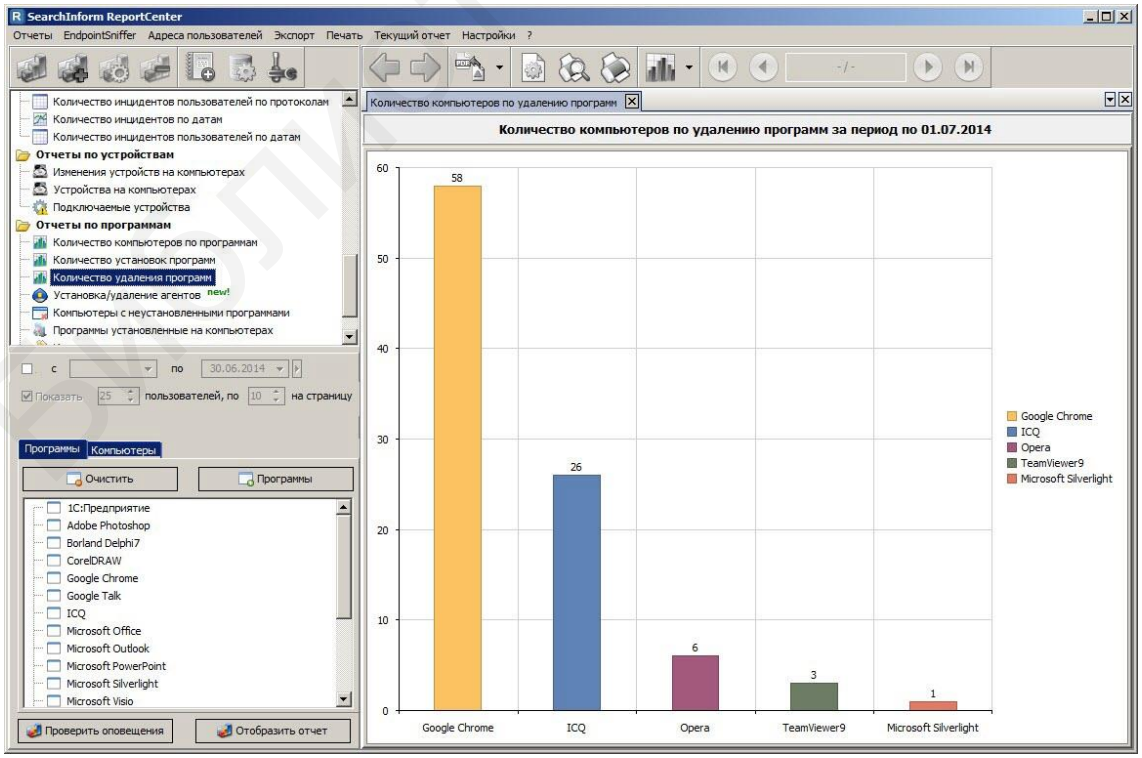


Рис. 3.116. Отчет «Количество удалений программ»

Библиотека БГУИР

Отчет «Компьютеры с неустановленными программами» отображает список компьютеров, на которых не установлены выбранные программы (рис. 3.117), отчет «Программы, установленные на компьютерах» – список программ, установленных на всех либо выбранных компьютерах (рис. 3.118). Отчет может быть отображен по определенным программам и/или с ограничением по времени.

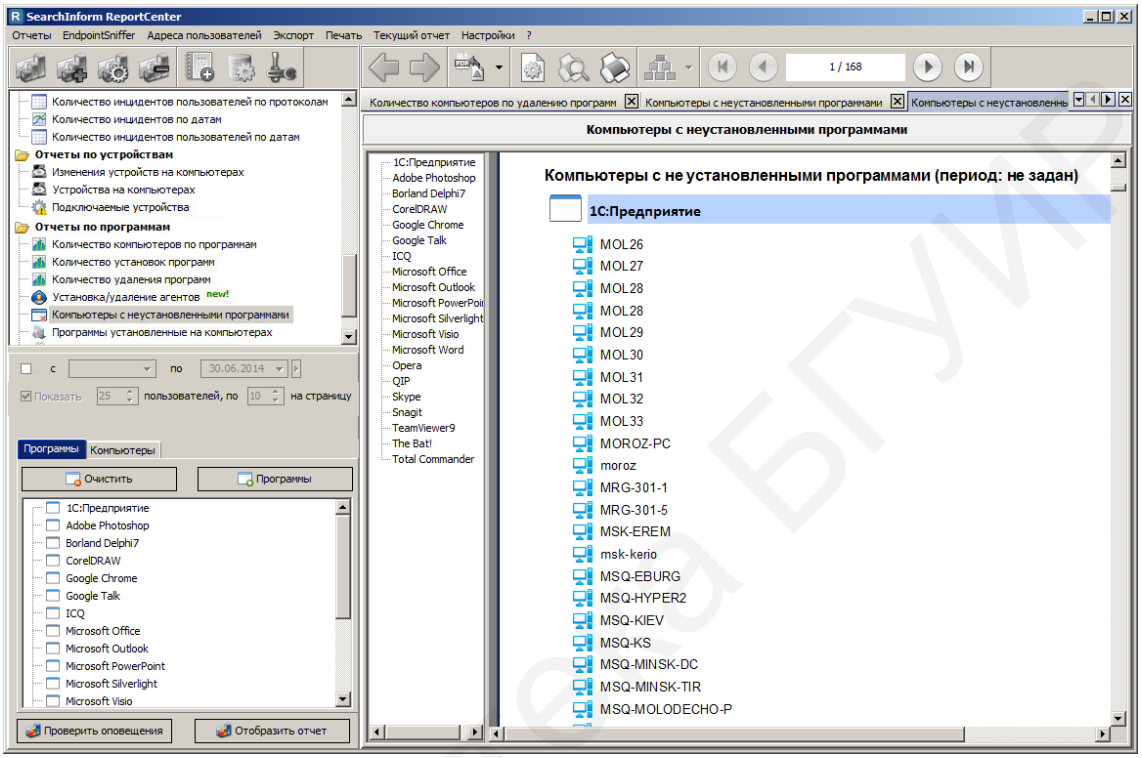


Рис. 3.117. Отчет «Компьютеры с неустановленными программами»

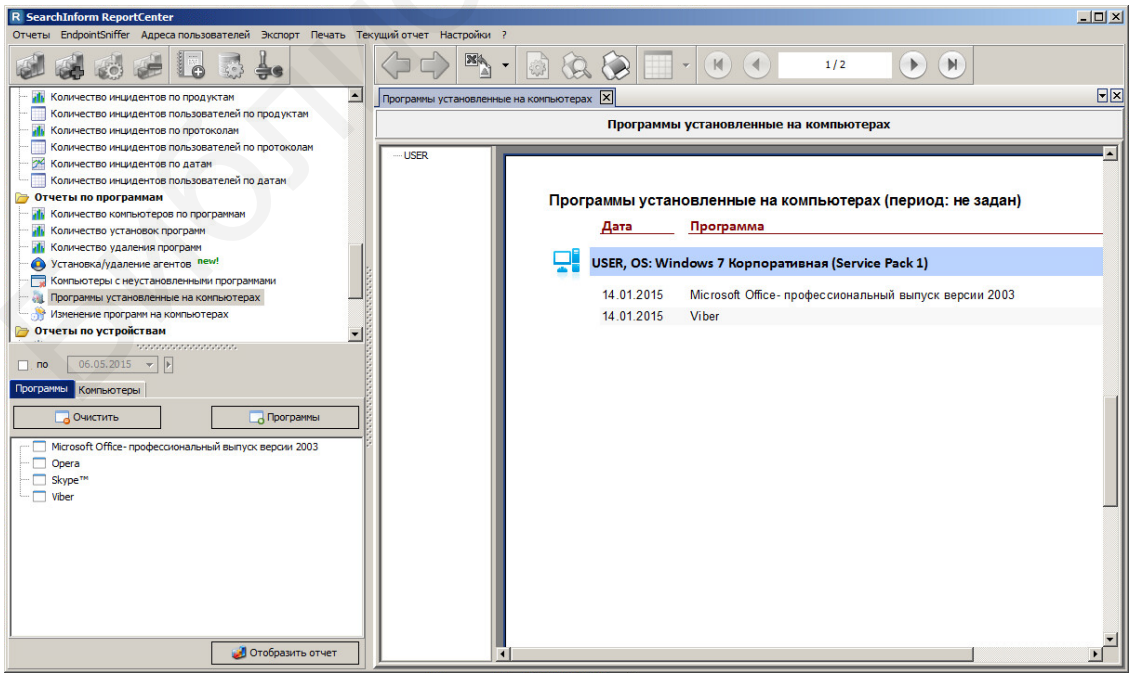


Рис. 3.118. Отчет «Программы, установленные на компьютерах»

Отчет «Изменение программ на компьютерах» отображает данные об истории установок/ удалений программ на выбранных компьютерах за заданный временной период (рис. 3.119).

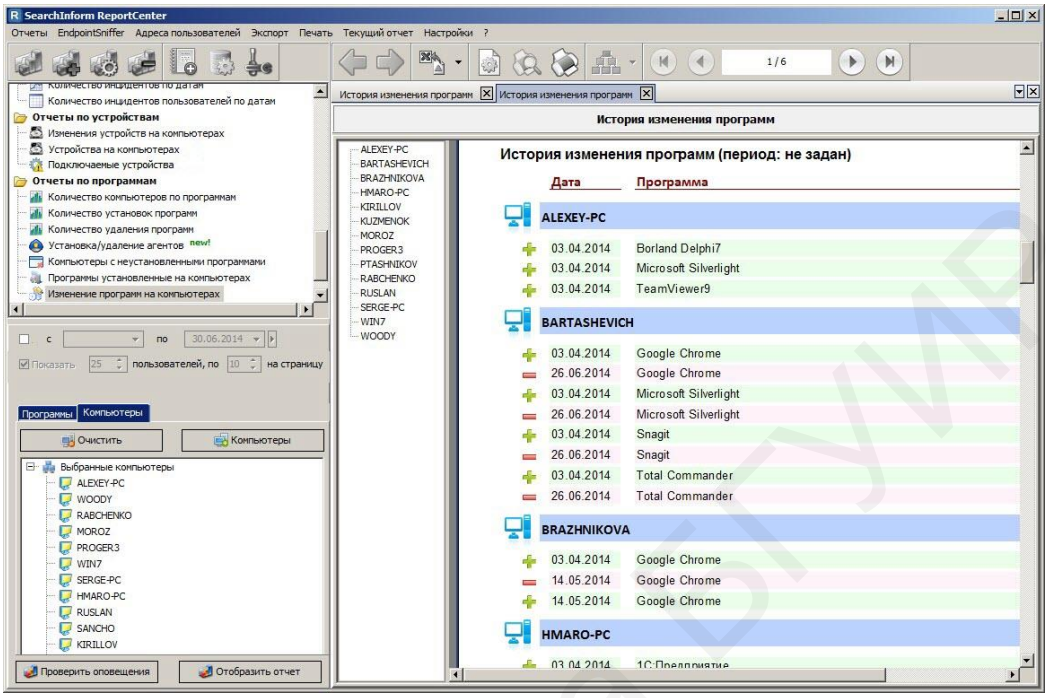


Рис. 3.119. Отчет «Изменение программ на компьютерах»

Отчеты ProgramSniffer. Подключение к базе данных компонента ProgramSniffer позволяет выводить следующие отчеты.

1. Отчет, отражающий суммарное время работы пользователей (рис. 3.120).

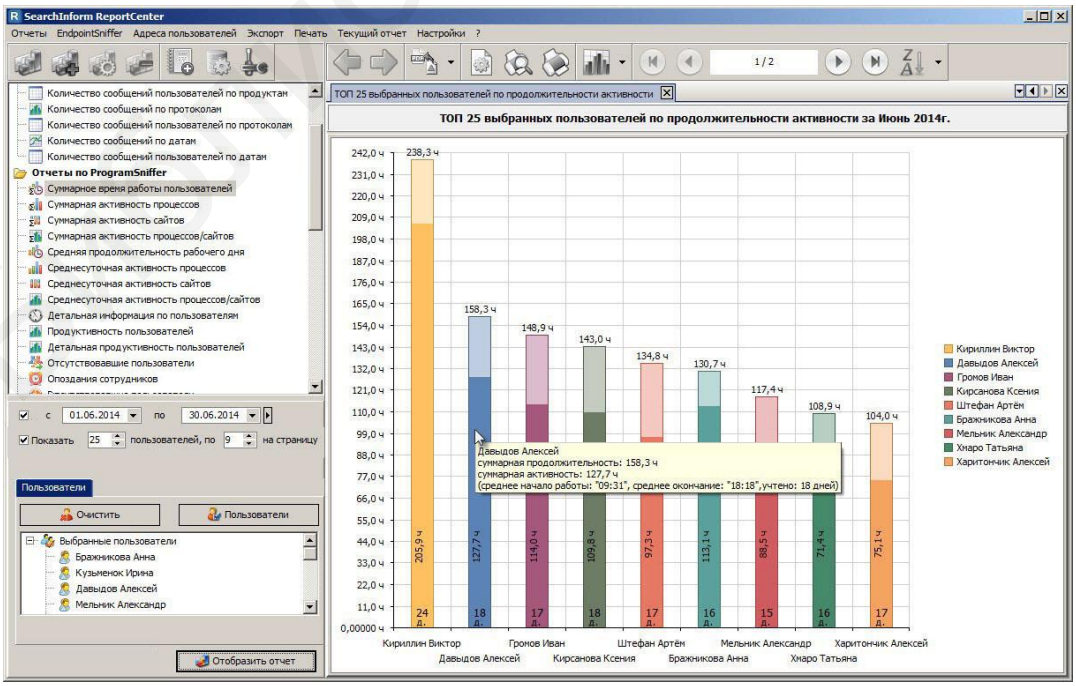


Рис. 3.120. Отчет «Суммарное время работы пользователей»

2. Отчет по суммарной активности процессов, запускаемых пользователями (рис. 3.121).

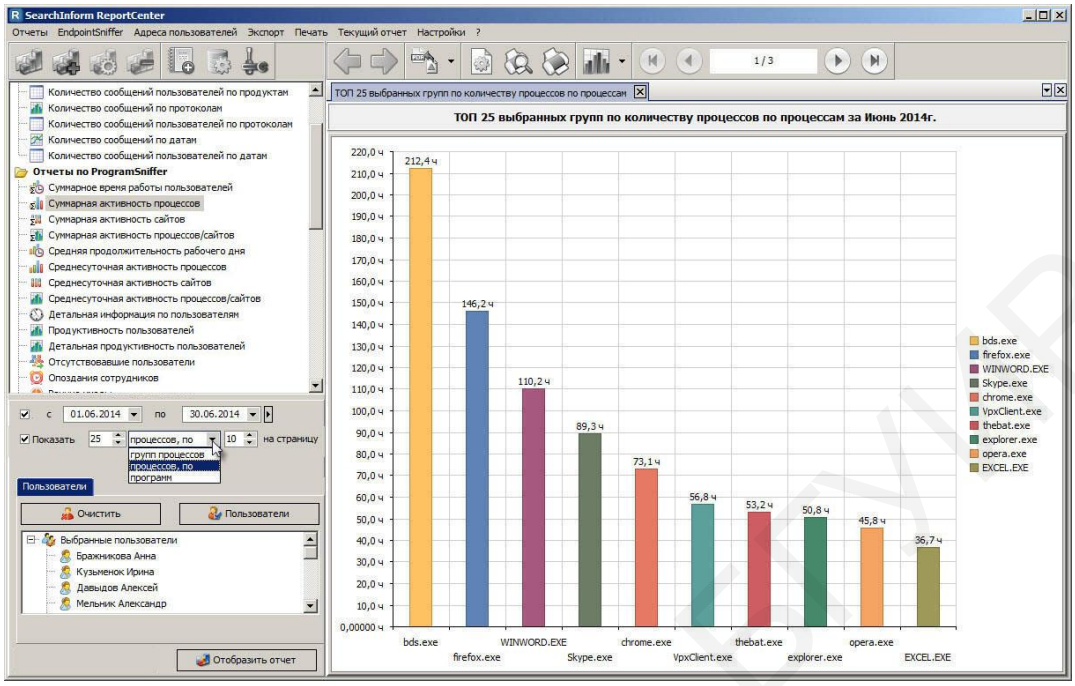


Рис. 3.121. «Суммарная активность процессов»

3. Отчет по суммарной активности сайтов (групп сайтов), посещаемых пользователями (рис. 3.122).

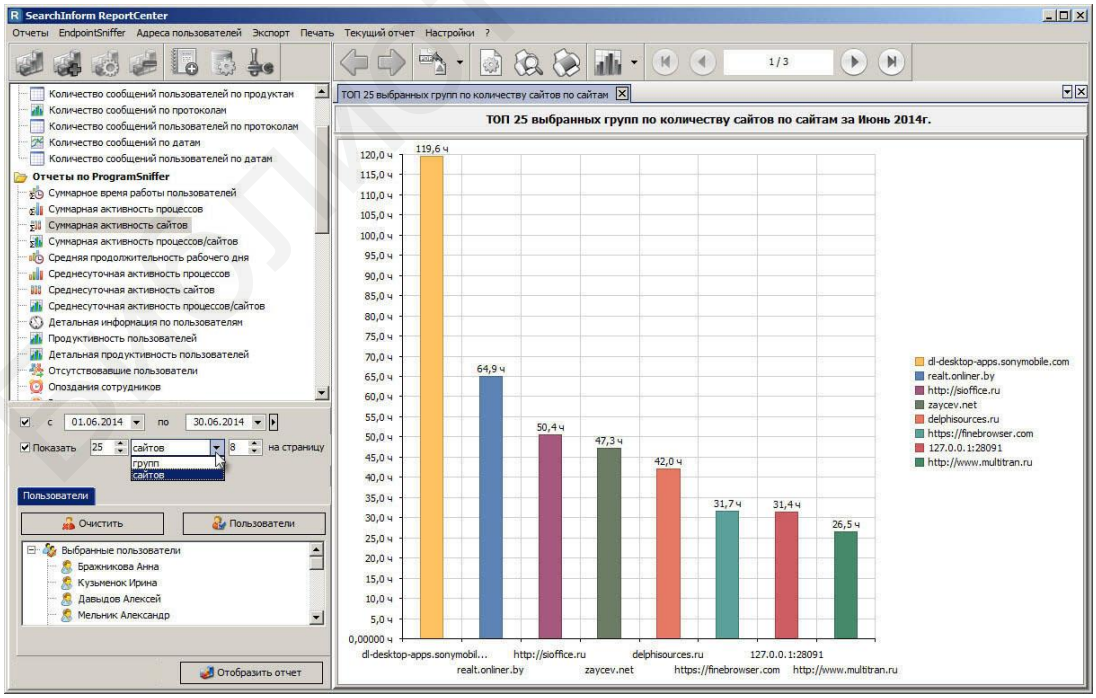


Рис. 3.122. Отчет «Суммарная активность сайтов»

4. Отчет по суммарной активности процессов (сайтов), запускаемых пользователями. Могут быть отображены как группы процессов, так и отдельные процессы и программы (рис. 3.123).

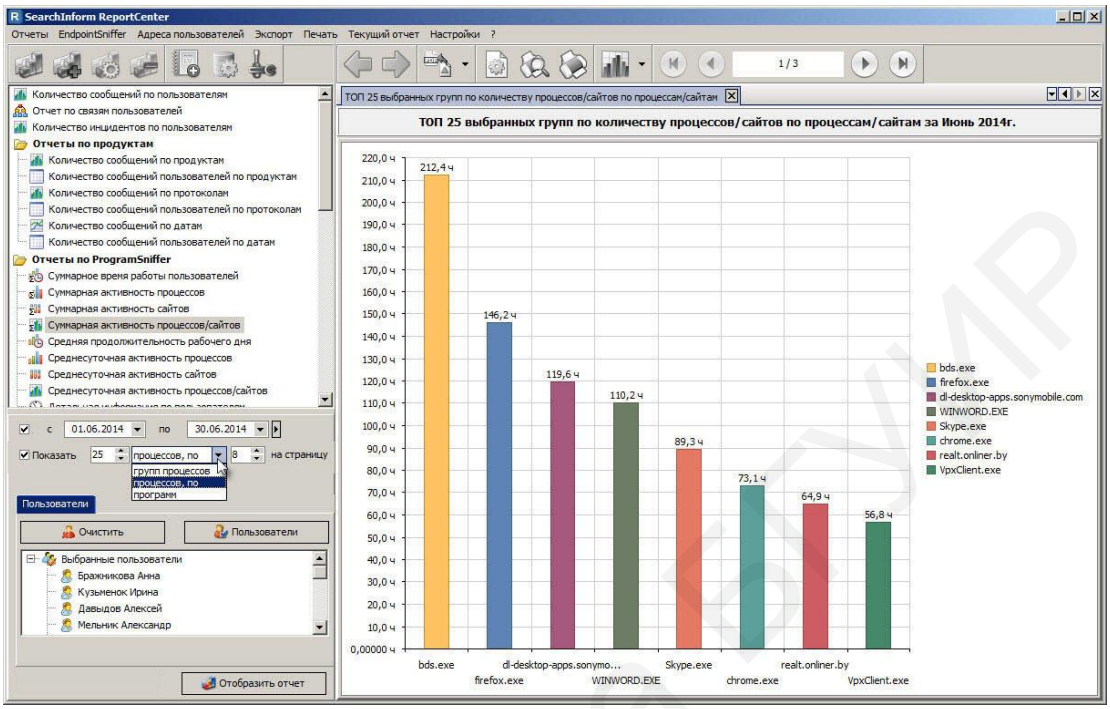


Рис. 3.123. Отчет «Суммарная активность процессов/сайтов»

5. Отчет по средней продолжительности рабочего дня пользователей (рис. 3.124).

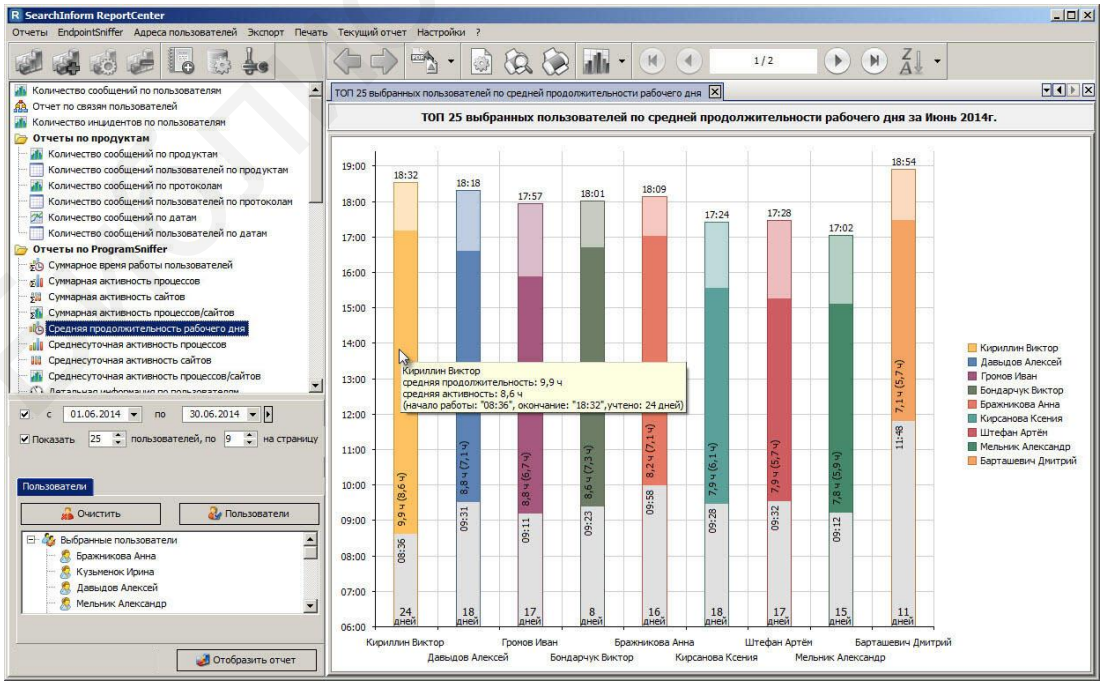


Рис. 3.124. Отчет «Средняя продолжительность рабочего дня»

6. Отчет по среднесуточной активности процессов, запускаемых пользователями (рис. 3.125).

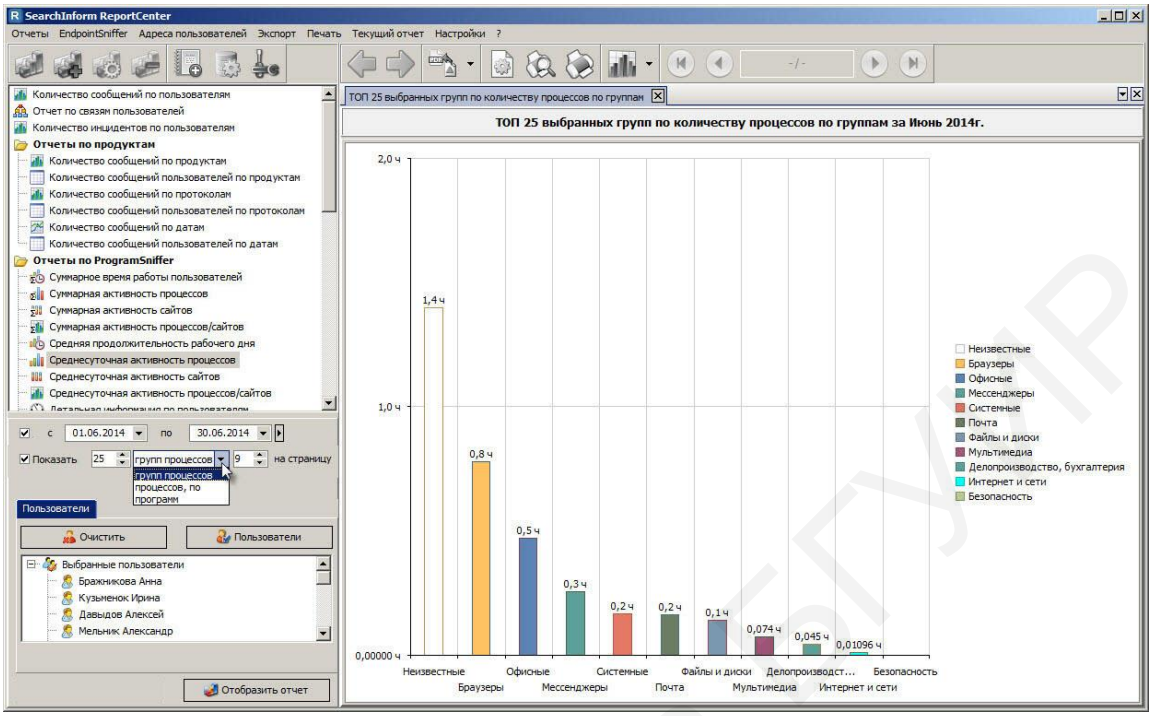


Рис. 3.125. Отчет «Среднесуточная активность процессов»

7. Отчет по средней суточной активности сайтов (групп сайтов), посещаемых пользователями (рис. 3.126).

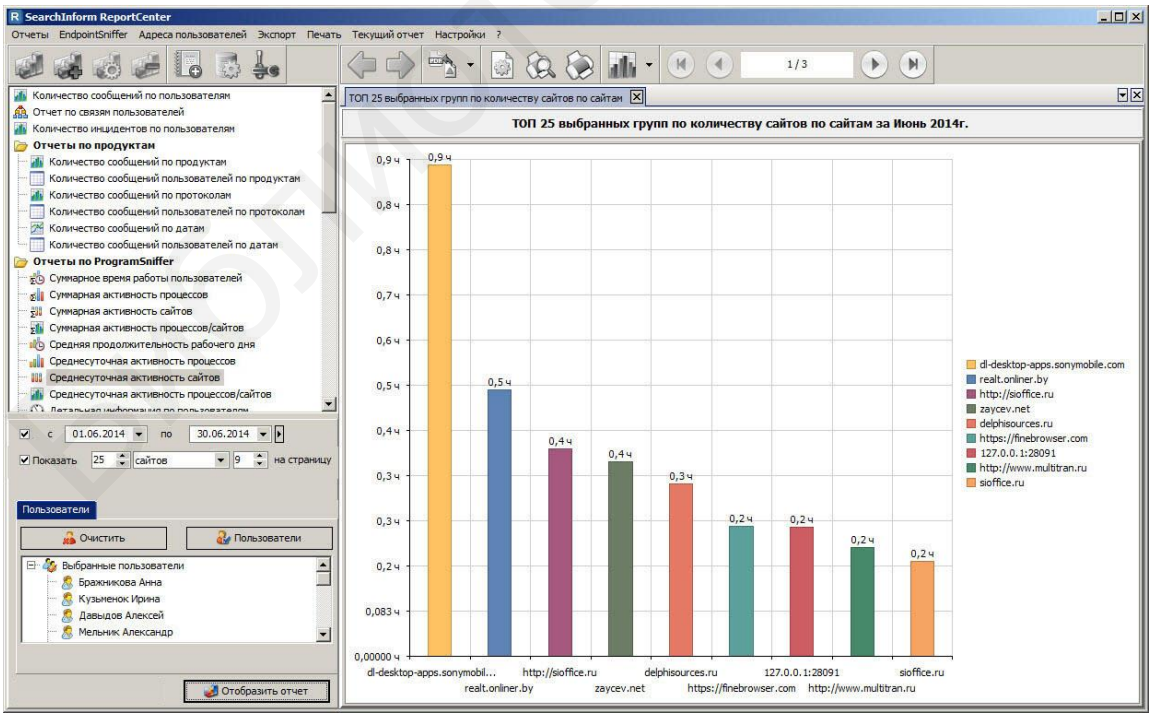


Рис. 3.126. Отчет «Среднесуточная активность сайтов»

8. Отчет по средней суточной активности процессов (сайтов), запускаемых пользователями. Могут быть отображены как группы процессов, так и отдельные процессы и программы (рис. 3.127).

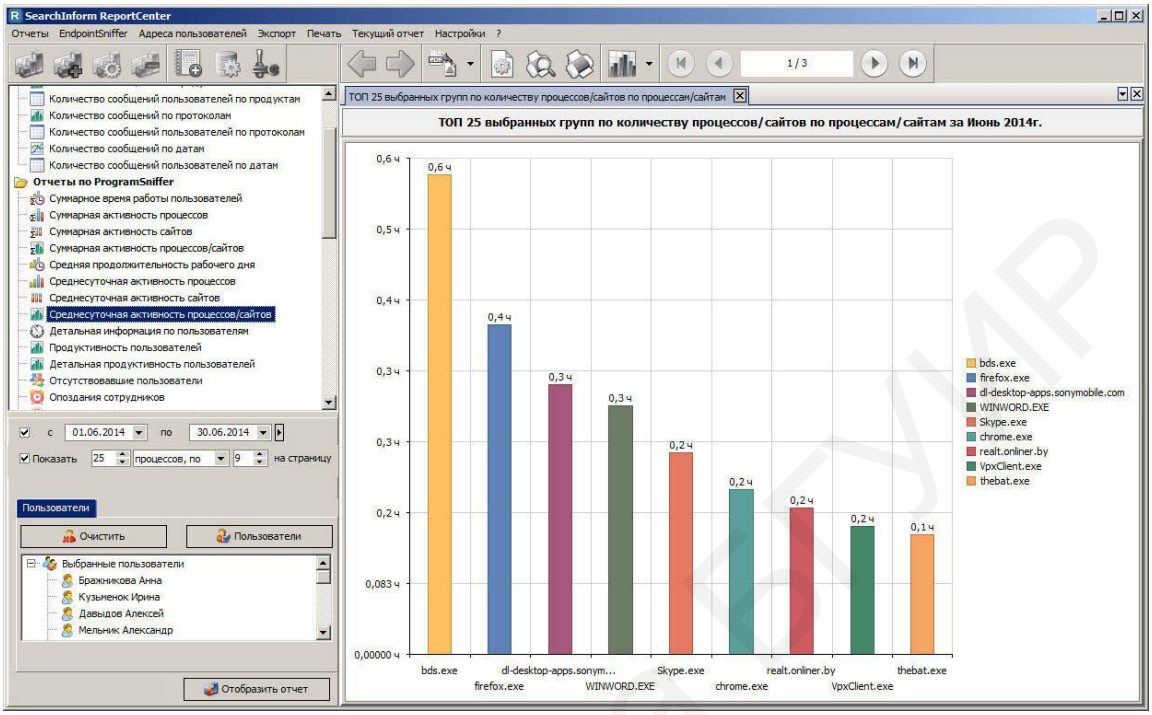


Рис. 3.127. Отчет «Среднесуточная активность процессов/сайтов»

9. Отчет, представляющий собой детальную информацию по пользователям (рис. 3.128).

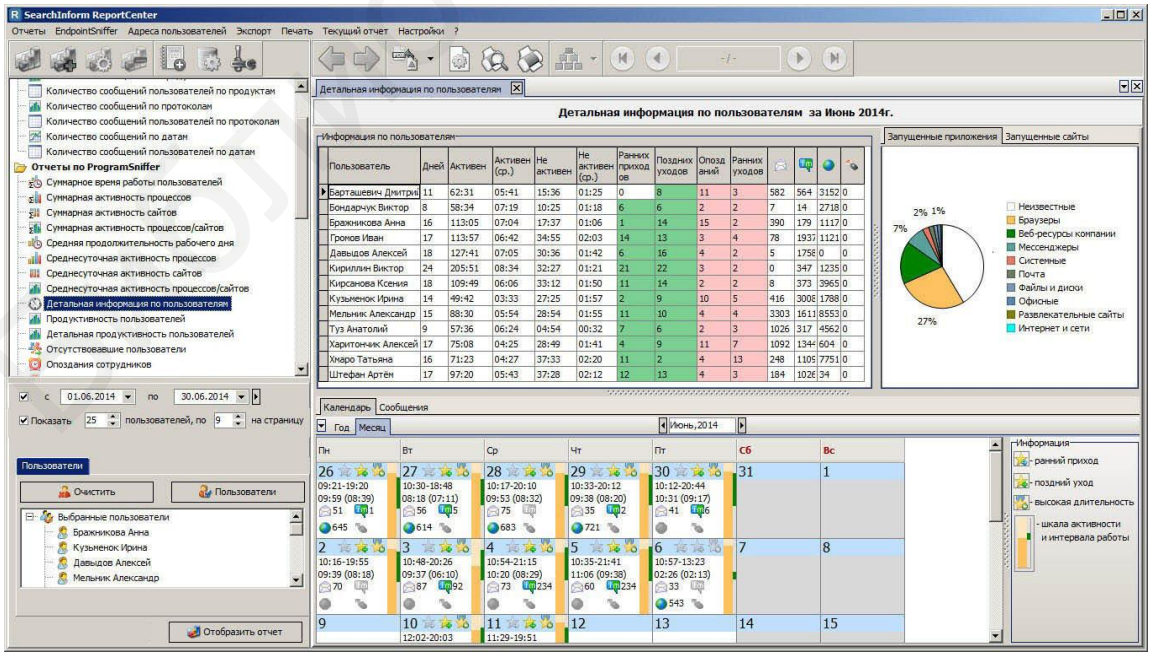


Рис. 3.128. Отчет «Детальная информация по пользователям»

10. Отчет «Отсутствовавшие пользователи», позволяющий просматривать статистические данные рабочего времени выбранных пользователей за заданный период (рис. 3.129).

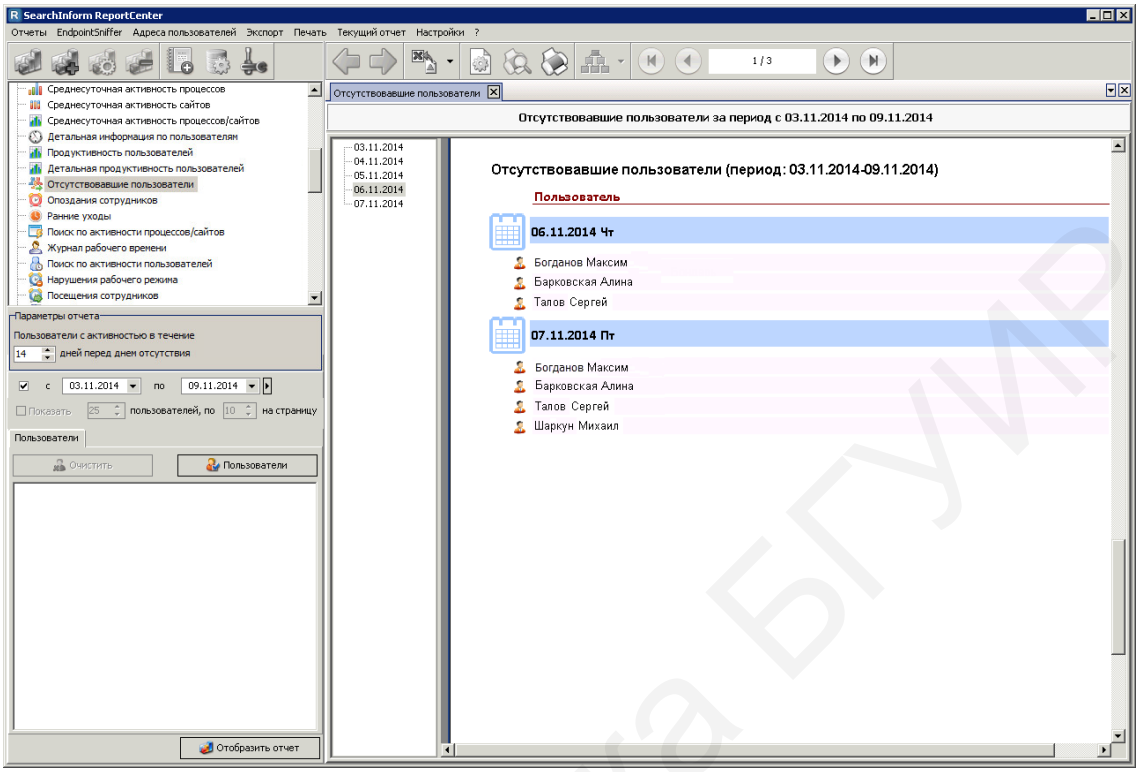


Рис. 3.129. Отчет «Отсутствовавшие пользователи»

11. Отчет «Опоздания сотрудников», позволяющий просматривать данные об опозданиях выбранных пользователей за указанный период времени (рис. 3.130).

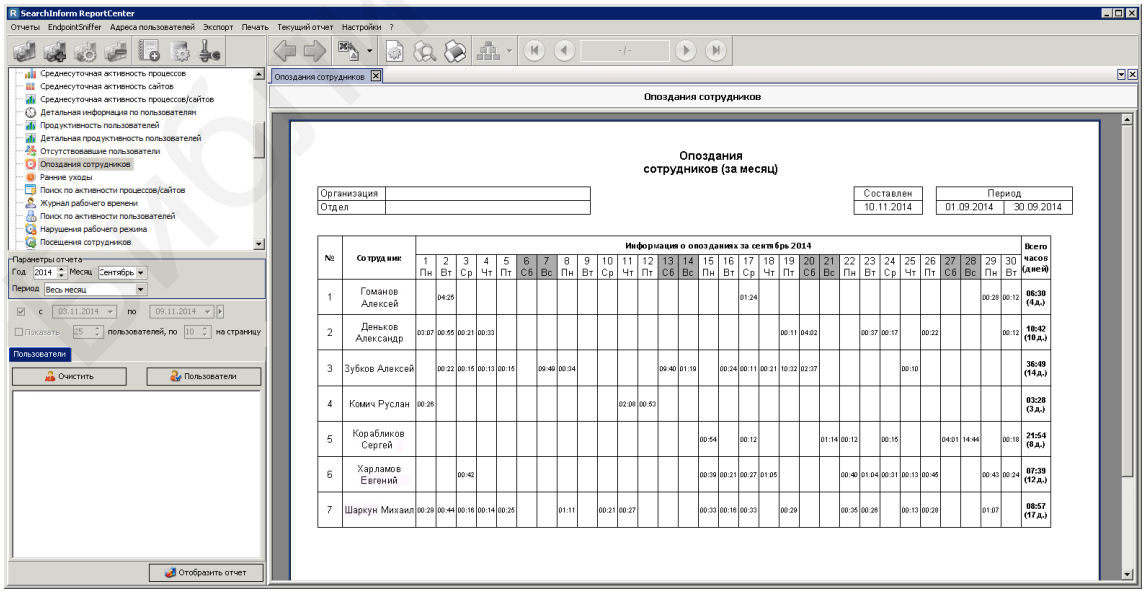


Рис. 3.130. Отчет «Опоздания сотрудников»

Библиотека БГУИР

12. Отчет «Ранние уходы», отображающий данные о выбранных пользователях, которые покидали рабочие места раньше положенного времени за указанный период времени (рис. 3.131).

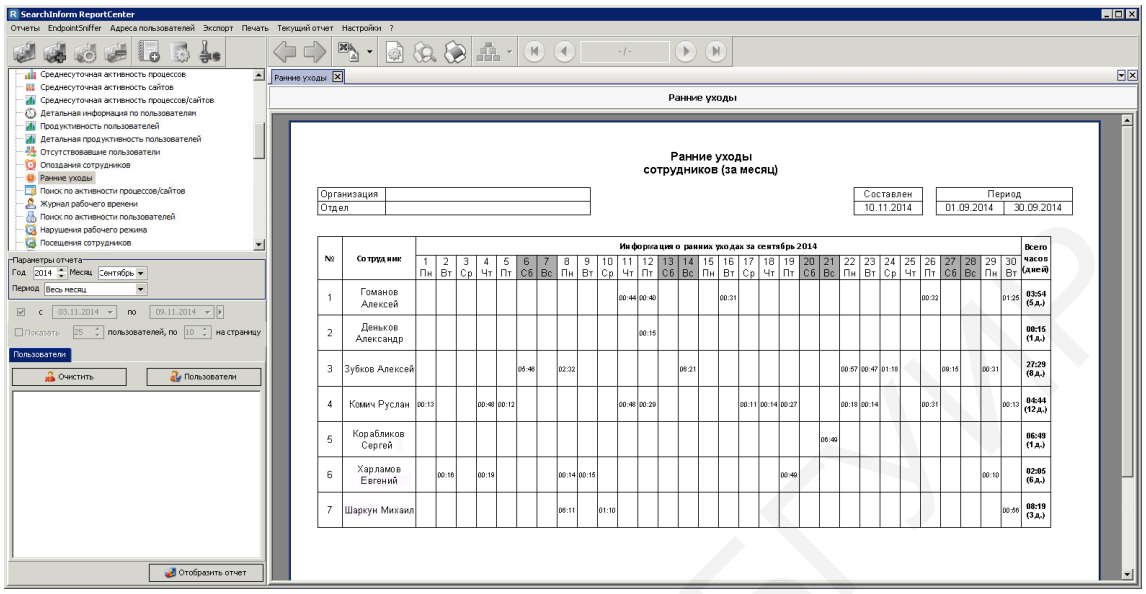


Рис. 3.131. Отчет «Ранние уходы»

13. Отчет, представляющий собой оповещения, связанные с длительной работой пользователей в приложениях, не связанных с рабочей деятельностью (рис. 3.132).

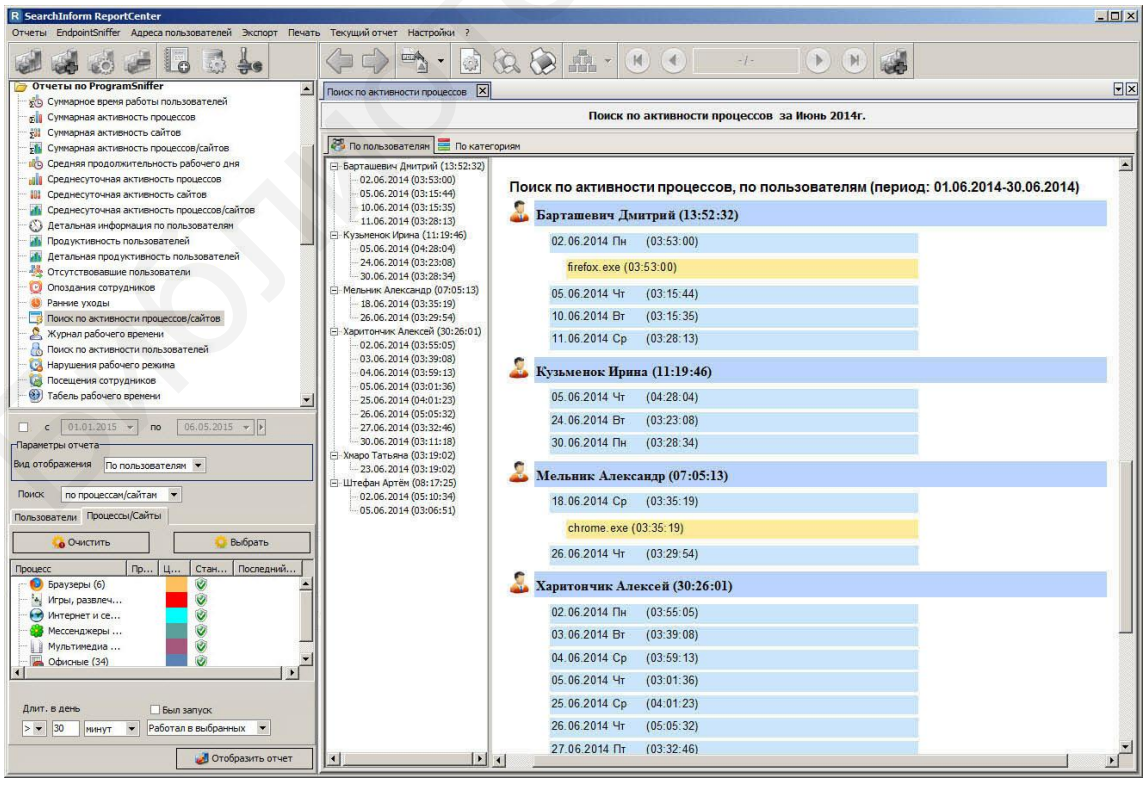


Рис. 3.132. Отчет «Поиск по активности процессов/сайтов»

Для отображения в отчете информации только по интересуемым процессам необходимо сделать предварительные настройки. На вкладке «Процессы/Сайты» нажмите кнопку «Выбрать» (рис. 3.133).

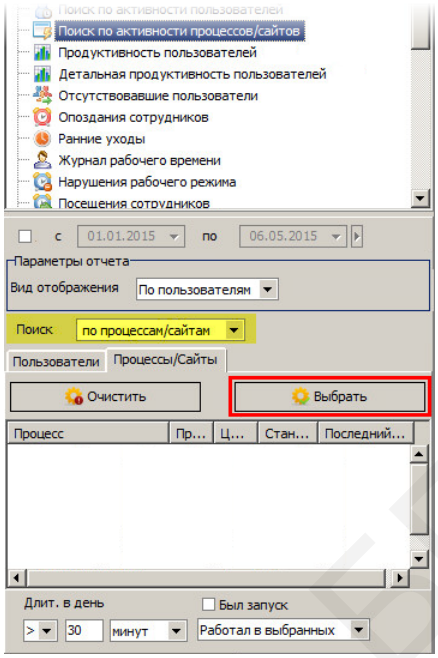


Рис. 3.133. Выбор процессов и групп

В диалоговом окне «Выбор процессов и групп» разверните требуемую группу процессов и, выделив интересующие вас процессы, перенесите их в правую часть окна с помощью кнопки мыши. Группа процессов также может быть перенесена целиком (рис. 3.134).

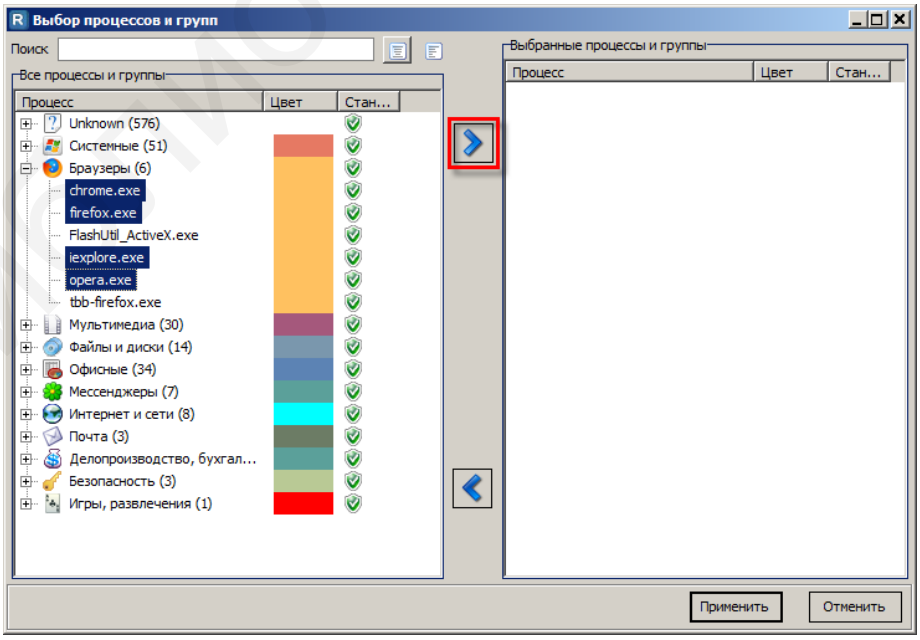


Рис. 3.134. Добавление процессов/групп

Библиотека БГУИР

Дополнительно настройте следующие параметры (рис. 3.135):

– «Длит. в день» – укажите минимальную или максимальную суточную продолжительность времени работы в выбранной группе/приложении; в случае, если поиск производится за несколько дней или месяцев, в результаты запроса попадут все рабочие дни, в которые группа/приложения использовались с указанной длительностью;

– «Был запуск» – установите флажок, если вам интересен сам факт запуска данного приложения;

– выпадающий список «Работал в выбранных»/«Кроме выбранных» – поиск может быть произведен с учетом выбранных групп/процессов либо игнорируя указанные (поиск будет произведен по всем остальным группам/процессам, кроме указанных).

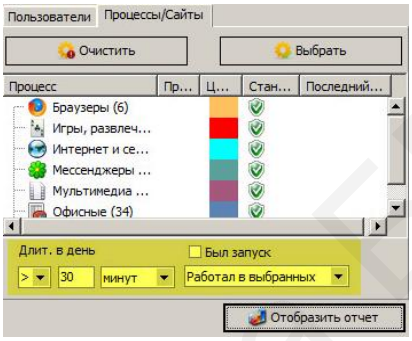


Рис. 3.135. Дополнительные параметры

14. Отчет «Журнал рабочего времени», позволяющий просматривать статистические данные рабочего времени выбранных пользователей за заданный период (рис. 3.136).

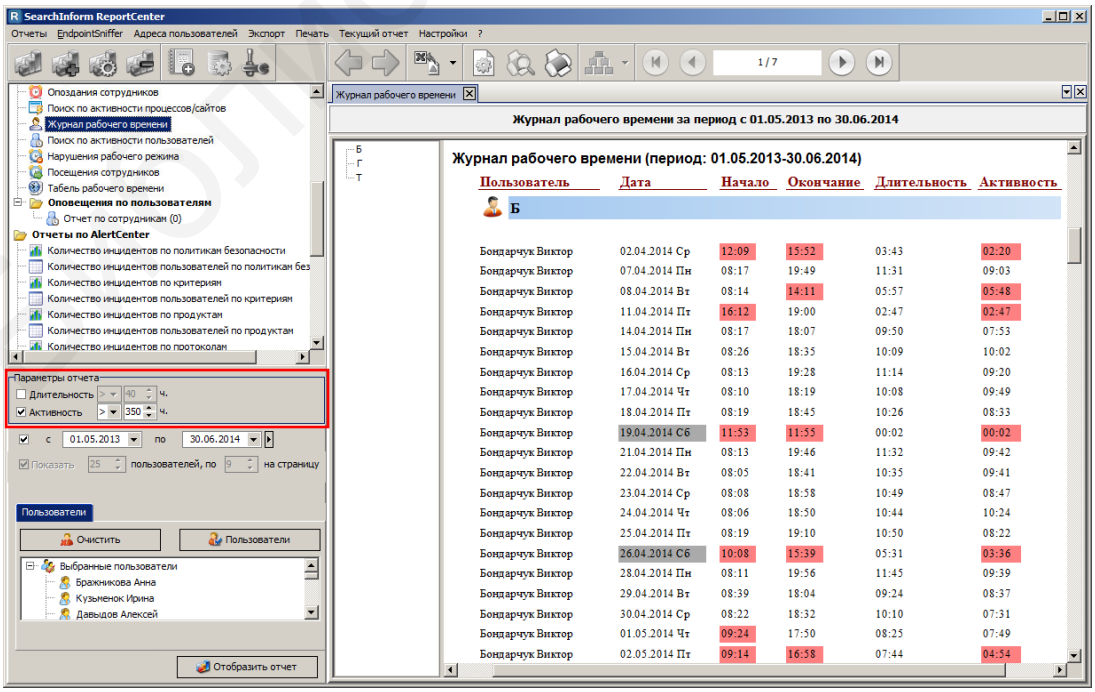


Рис. 3.136. Отчет «Журнал рабочего времени»

15. Отчет, отображающий оповещения, связанные с недостаточной активностью пользователей в рабочее время (рис. 3.137).

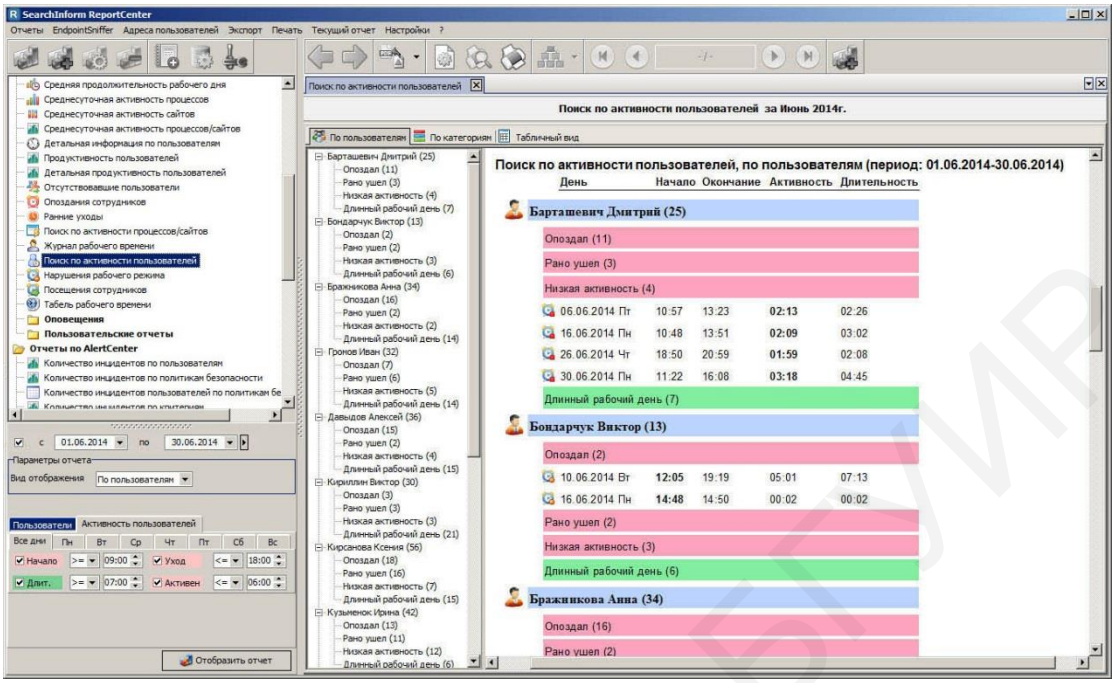


Рис. 3.137. Поиск по активности пользователей

Для корректного отображения оповещений по активности пользователей необходимо сделать предварительные настройки.

На вкладке «Активность пользователей» установите диапазон рабочего времени по дням недели согласно графику работы вашей компании (параметры «Начало» и «Уход»), а также продолжительность рабочего дня без учета обеда (параметр «Длит.») (рис. 3.138).

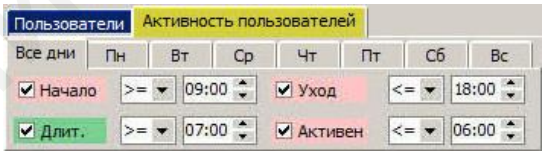


Рис. 3.138. Выбор дополнительных параметров

В параметре «Активен» укажите продолжительность времени активности сотрудника в течение рабочего дня (в идеале).

16. Отчет «Нарушения рабочего режима», позволяющий просматривать данные о нарушениях рабочего режима, таких как опоздания и низкая активность (рис. 3.139).

Библиотека БГУИР

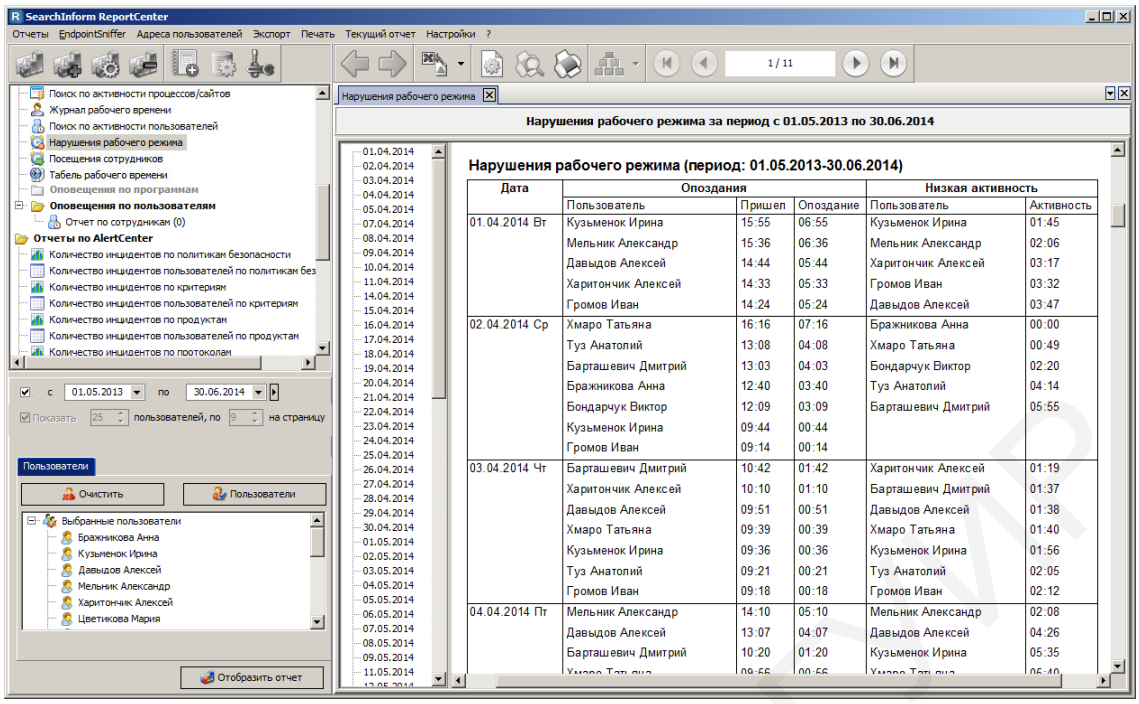


Рис. 3.139. Отчет «Нарушения рабочего режима»

17. Отчет «Посещения сотрудников», позволяющий просматривать график приходов пользователей на работу в течение заданного периода времени (рис. 3.140).

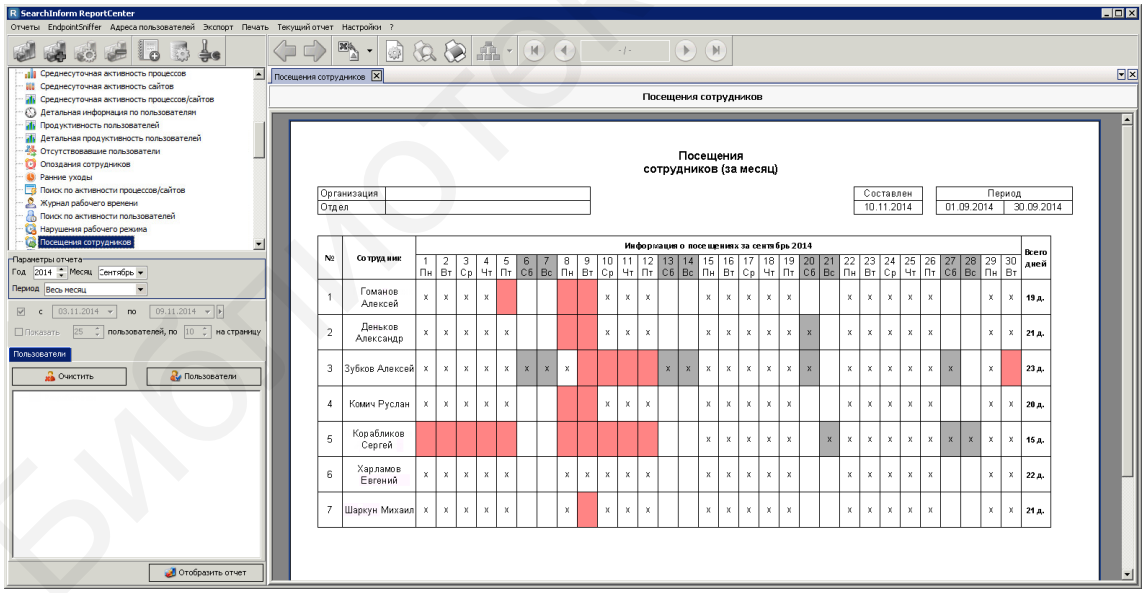


Рис. 3.140. Отчет «Посещения сотрудников»

18. Отчет «Табель рабочего времени», позволяющий просматривать информацию о приходах, уходах и отработанном времени выбранных пользователей за заданный период (рис. 3.141).

Библиотека ВГУИР

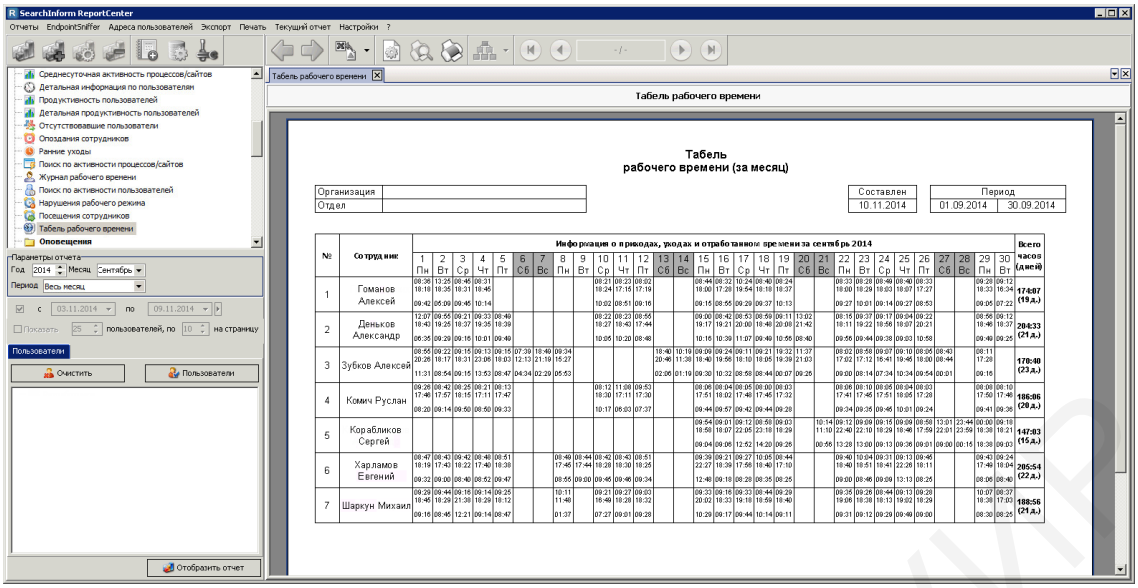


Рис. 3.141. Отчет «Табель рабочего времени»

3.4. Ведение полноформатного расследования в рамках консоли IncidentCenter

SearchInform IncidentCenter предоставляет возможность ведения сотрудником службы ИБ полноформатного расследования инцидентов в одной консоли (рис. 3.142). Приложение позволяет работать с делами и прикрепленными к ним файлами, группировать дела по папкам, просматривать списки фигурантов и др.

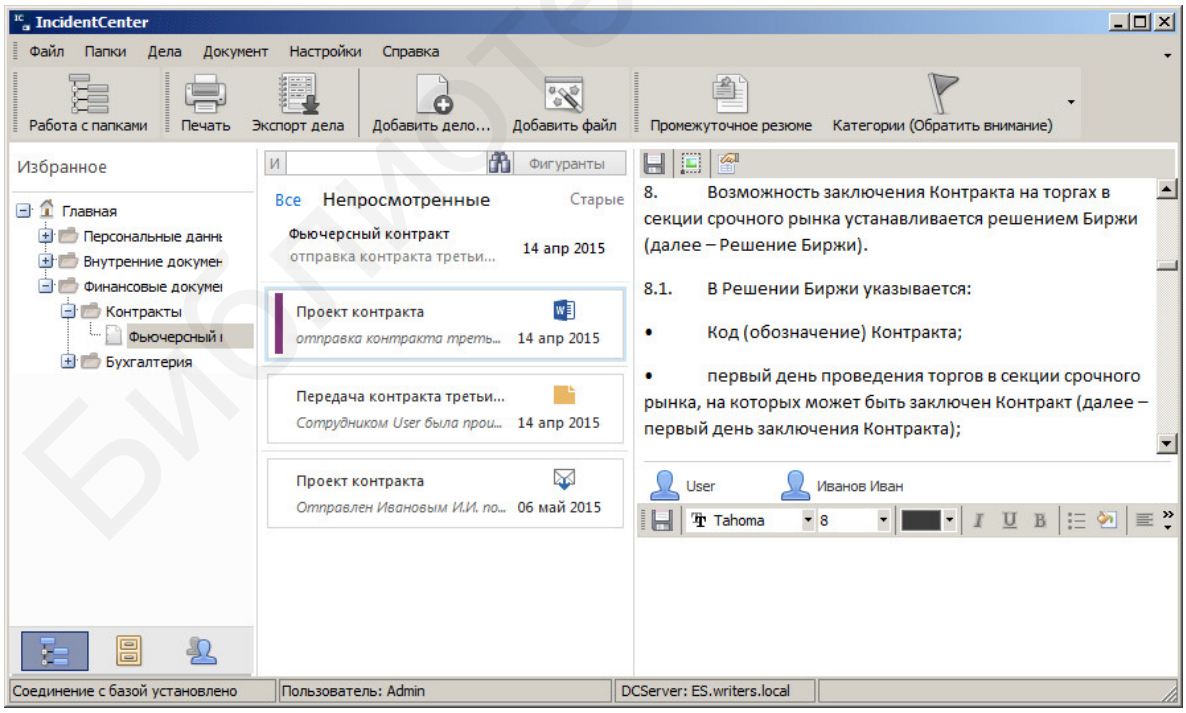


Рис. 3.142. Консоль IncidentCenter

Библиотека БГУИР

Консоль IncidentCenter выполняет следующие функции:
– работа с папками;
– добавление дел;
– добавление файлов к делам;
– работа с архивом дел;
– работа со списком фигурантов по делам;
– настройка категорий файлов;
– просмотр истории изменений;
– настройка списка допусков.

Работа с папками. Для работы с папками используется одноименная кнопка (рис. 3.143).

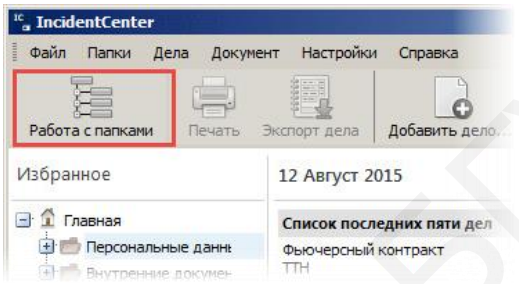


Рис. 3.143. Работа с папками

На вкладке «Общие» редактируется дерево папок. Папки можно создавать, удалять (дела из удаленных папок перемещаются в архив), перетаскивать в другие папки (drag-and-drop), а также просматривать информацию о выбранной папке (в правой части окна) (рис. 3.144).

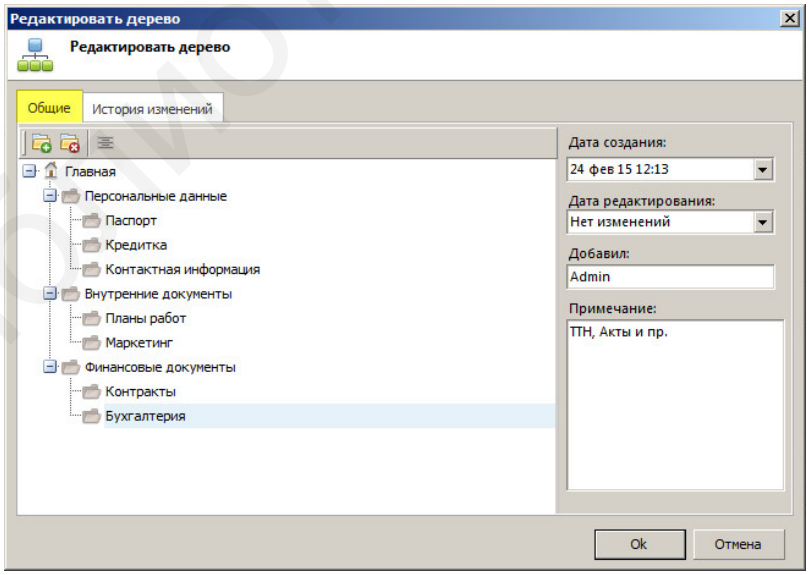


Рис. 3.144. Редактирование дерева папок

На вкладке «История изменений» отображаются данные по последним изменениям выбранной папки.

Библиотека БГУИР

Для *добавления новой папки* укажите область в дереве, куда она будет добавлена (в корень директории или внутрь любой другой папки*), затем воспользуйтесь командой меню «Папки» → «Добавить папку» либо контекстным меню «Добавить папку», вызываемым щелчком правой кнопки мыши. Также папки можно добавлять при помощи кнопки «Работа с папками» (рис. 3.145).

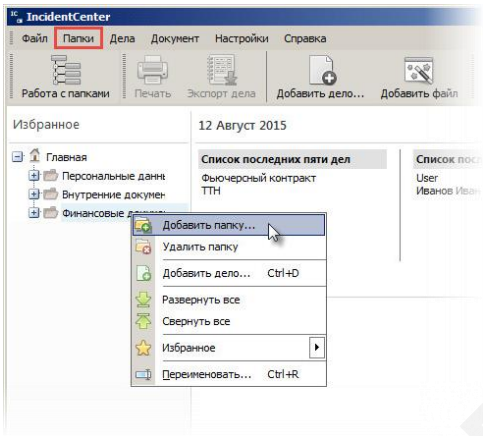


Рис. 3.145. Добавление папки

Введите название папки, а также при необходимости дополнительную информацию в поле «Примечание» (рис. 3.146).

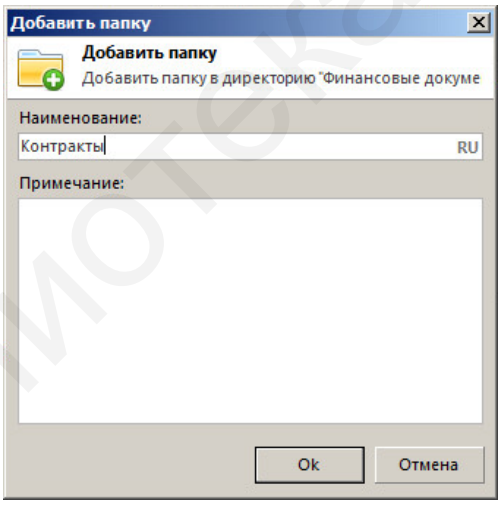


Рис. 3.146. Создание папки

Для удаления папки воспользуйтесь командой меню «Папки» → «Удалить папку» либо контекстным меню «Удалить папку», вызываемым щелчком правой кнопки мыши. Дела из удаляемых папок перемещаются в архив.

Для добавления дела выберите папку, в которую дело будет добавлено, затем воспользуйтесь командой меню «Дела» → «Добавить дело» либо контекстным меню «Добавить дело», вызываемым правой кнопки мыши (рис. 3.147).

* Максимальный уровень вложений папок – 2. Если текущий уровень вложения выше, то программа автоматически переведет добавляемую папку на уровень выше.

Библиотека БГУИР

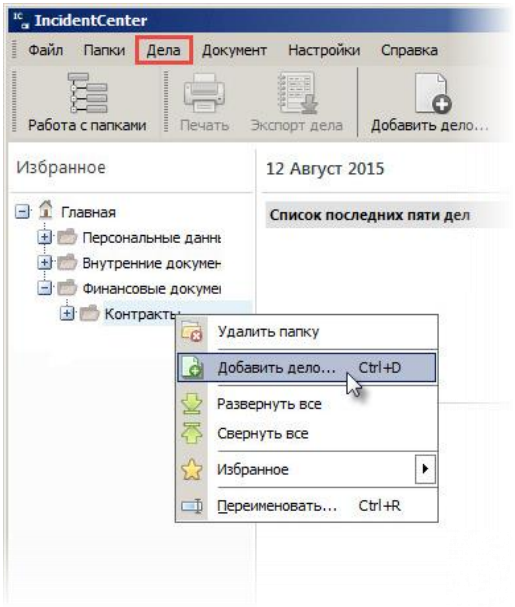


Рис. 3.147. Контекстное меню «Добавление дела»

Введите название дела, выберите папку (для создания новой – воспользуйтесь кнопкой «Добавить папку...»), при необходимости заполните поле «Примечание» и выберите файл, который является основанием для заведения дела (рис. 3.148).

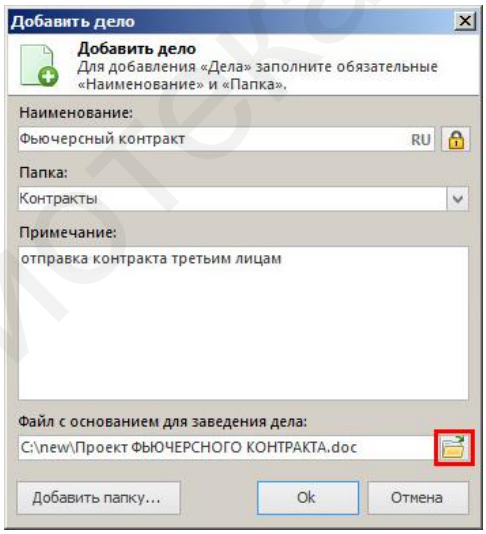


Рис. 3.148. Добавление дела

Для добавления файла воспользуйтесь кнопкой . В появившемся окне выберите требуемый файл. Дело будет добавлено в указанную папку (рис. 3.149).

Библиотека БГУИР

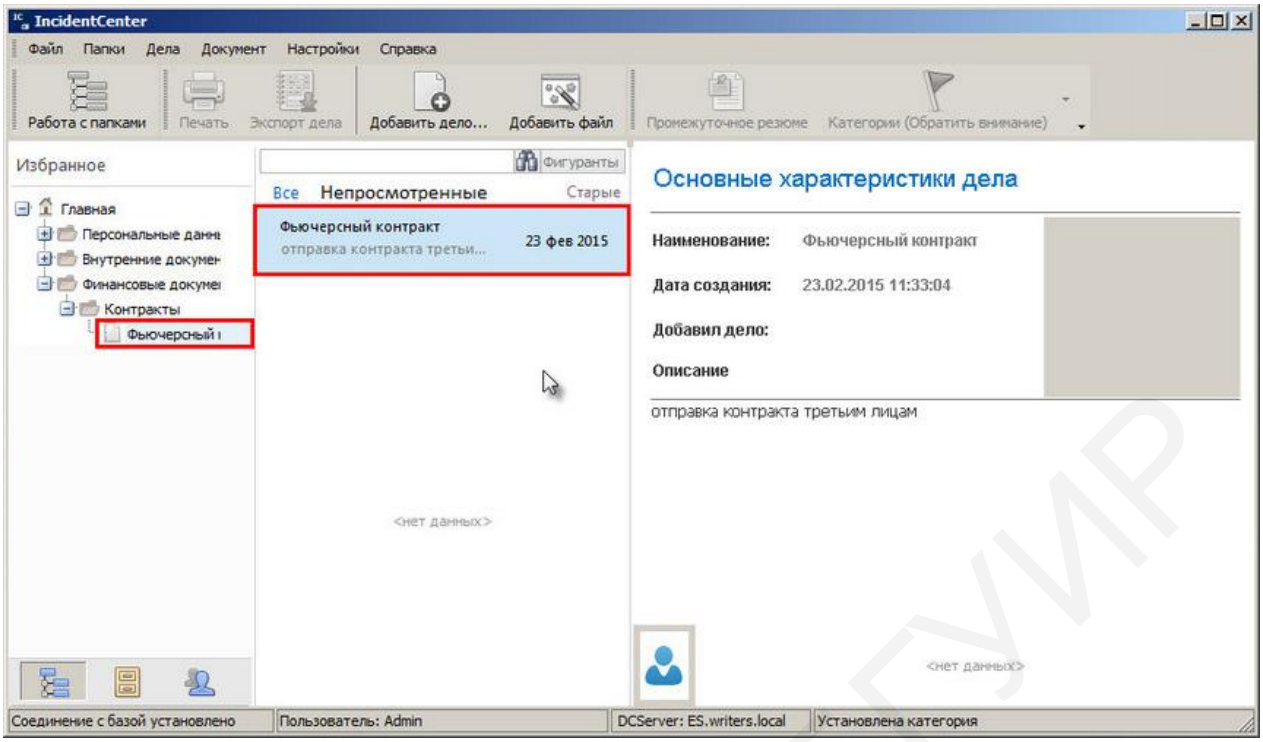


Рис. 3.149. Папка с вложенным делом

К созданным делам можно прикреплять файлы. Используйте кнопку «Добавить файл» (рис. 3.150).

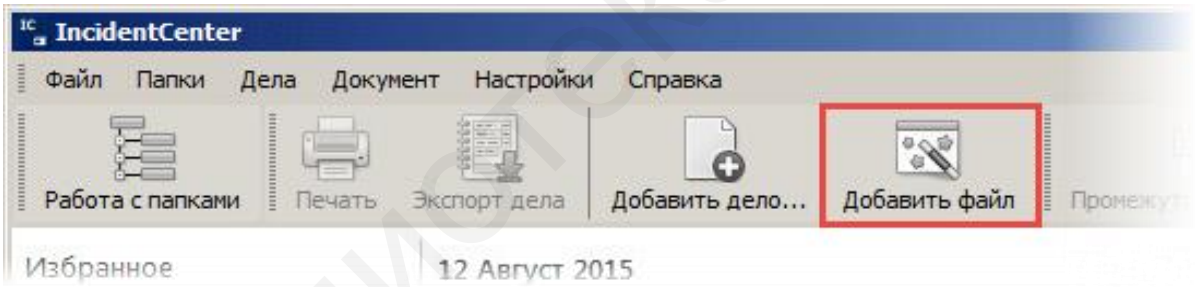


Рис. 3.150. Кнопка «Добавить файл»

Также файл можно добавить из окна результатов SearchInform Client при помощи команды контекстного меню «Добавить в IncidentCenter» (рис. 3.151).

В появившемся окне мастера добавления файлов выберите дело в списке папок, нажмите «Далее». При отсутствии необходимого дела добавьте новое при помощи кнопки «Добавить дело» (рис. 3.152).

В случае выбора в дереве папок/дел конкретного дела сразу откроется окно добавления описания к файлу.

Библиотека БГУИР

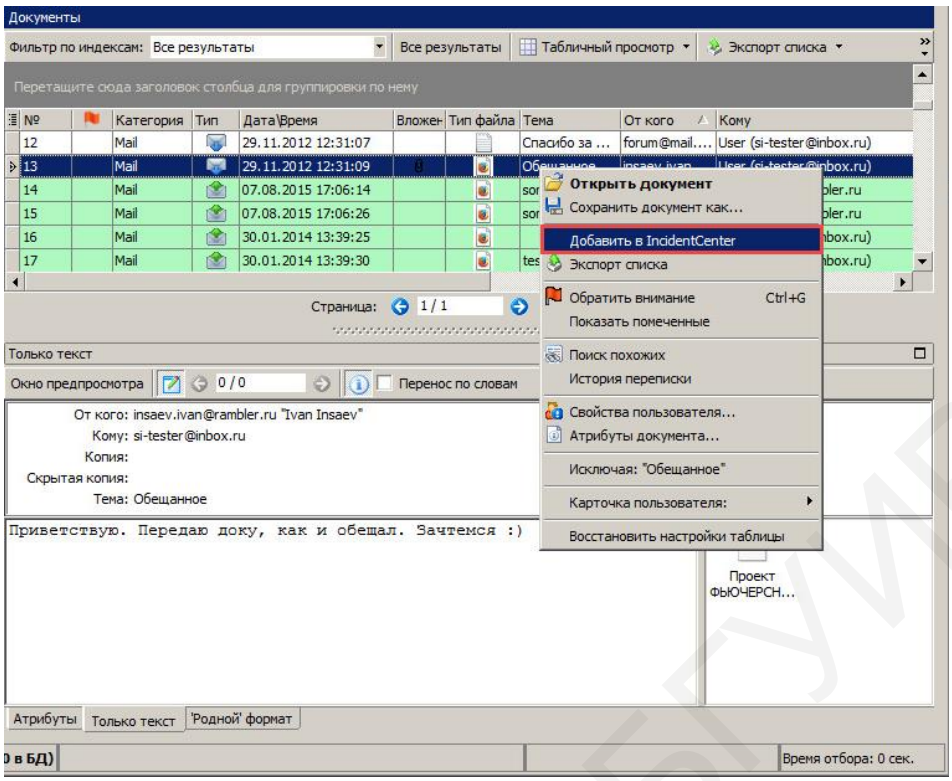


Рис. 3.151. Переход из SearchInform Client

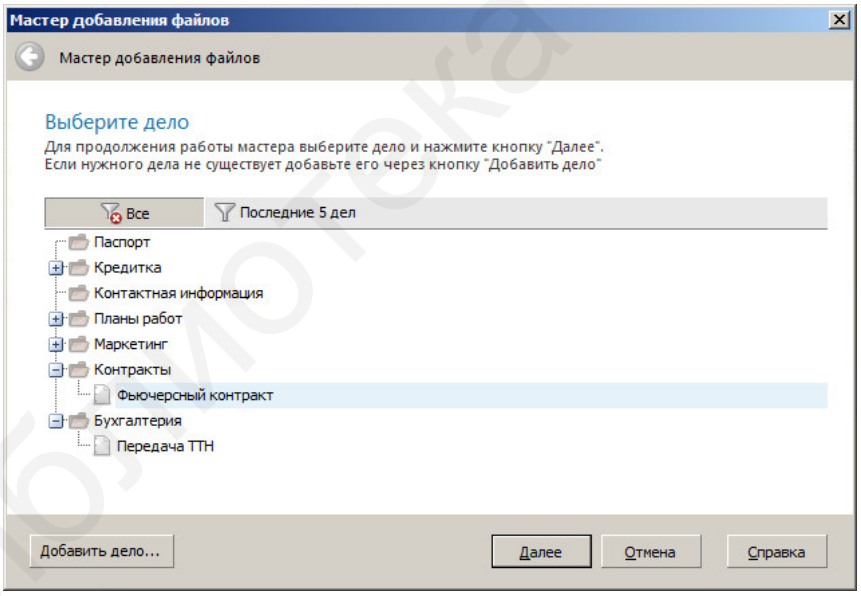


Рис. 3.152. Мастер добавления файлов

Задайте наименование файла и причину добавления в поле «Примечание», нажмите «Далее». Выберите файл в проводнике и нажмите «Финиш». Добавление файла будет завершено (рис. 3.153).

Библиотека БГУИР

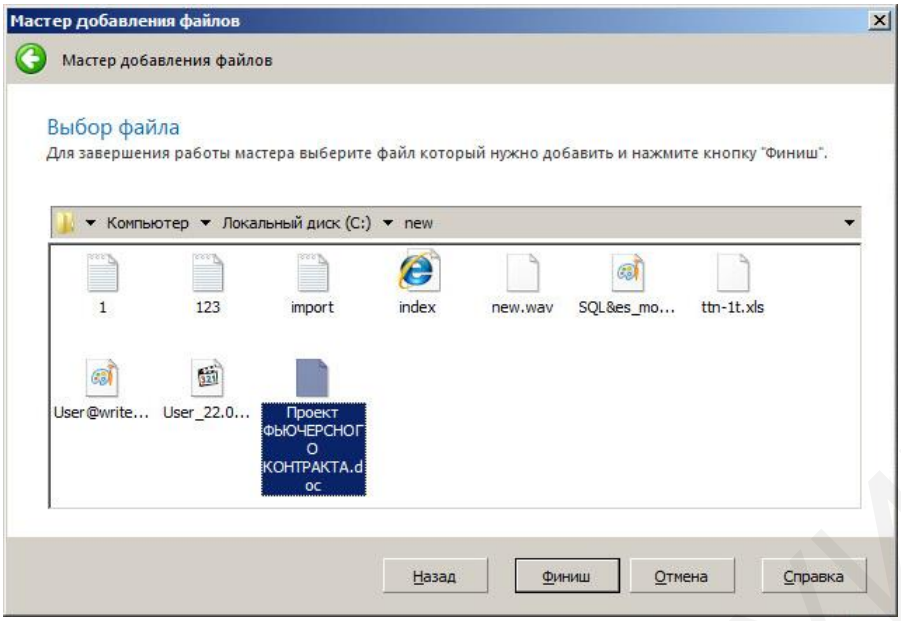


Рис. 3.153. Завершение добавления файла

Все закрытые дела перемещаются в архив. Для переноса дела в архив выделите в дереве дело, вызовите щелчком правой кнопки мыши контекстное меню и нажмите «Перенести в архив» (рис. 3.154).

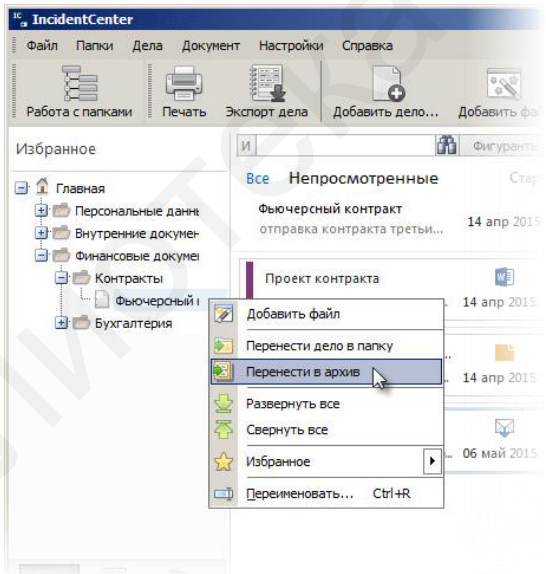


Рис. 3.154. Перенос дела в архив

В открывшемся окне укажите причину закрытия дела и нажмите «ОК». Находящиеся в архиве дела можно просмотреть с помощью кнопки  , находящейся в нижней части окна (рис. 3.155).

Библиотека БГУИР

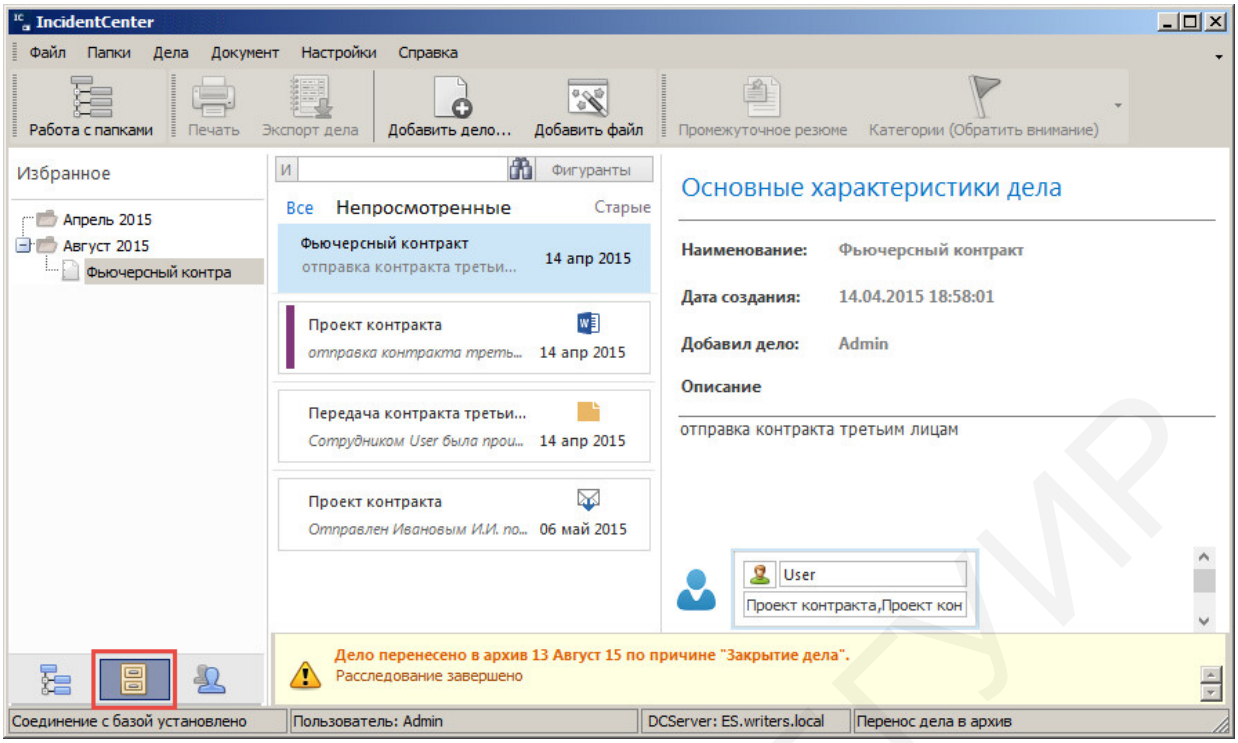


Рис. 3.155. Просмотр архива

Список фигурантов по делу отображает перечень людей, которые были связаны с прикрепленными к делам документами. Для переключения режима просмотра нажмите кнопку  в нижней части окна (рис. 3.156).

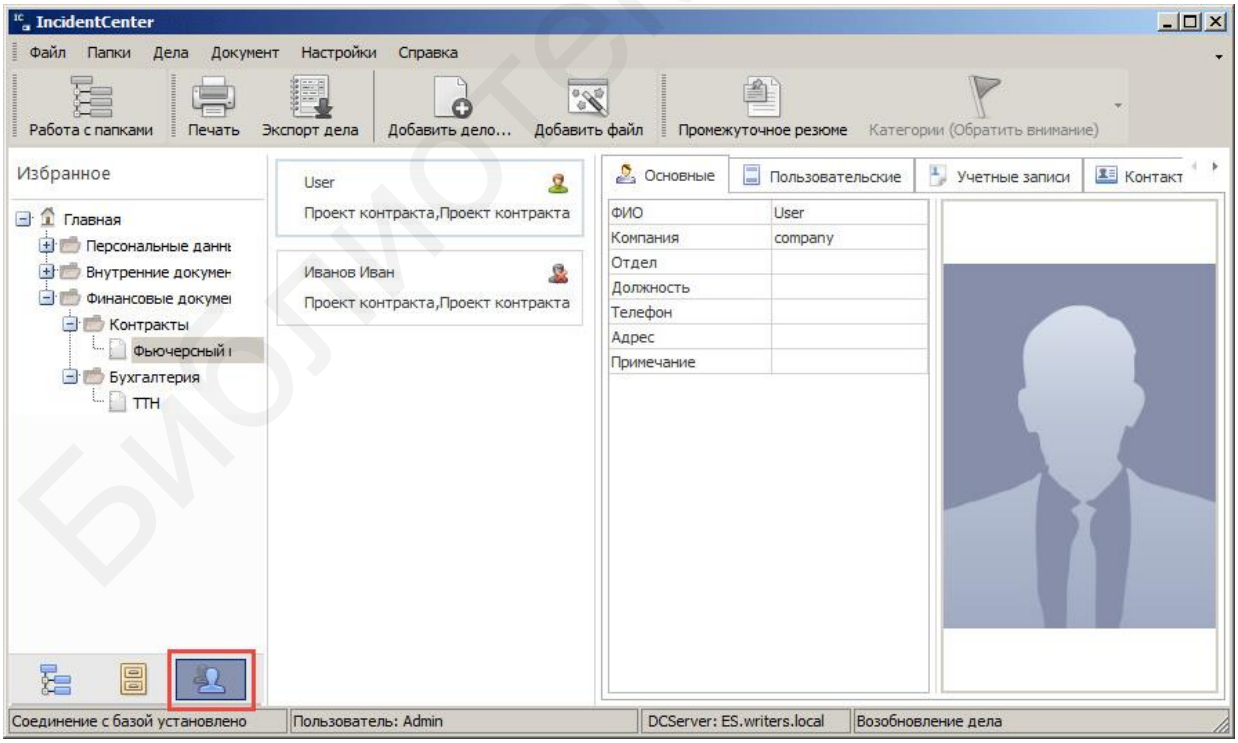


Рис. 3.156. Просмотр фигурантов дела

В правой части окна отображается информация из карточки пользователя SearchInform Client.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

Сегодня на рынке присутствует достаточно большое число продуктов, которые могут быть использованы для защиты конфиденциальных данных. Среди них имеются как специализированные решения для выполнения конкретных задач, так и комплексные системы, включающие в себя множество разнообразных функций. Одним из наиболее интересных и актуальных, с нашей точки зрения, типов подобных систем являются DLP-решения. Как было отмечено ранее, это не единственное, но наиболее распространенное название систем, предназначенных для минимизации рисков утечек конфиденциальных данных организации. Работа DLP-системы основывается на перехвате и анализе потоков данных (предполагаемых каналов утечек), которые циркулируют внутри либо пересекают периметр защищаемой (корпоративной) сети, что позволяет своевременно выявлять несанкционированные действия с конфиденциальной информацией, пресекать такие действия, а также помогает в сборе доказательств и расследовании инцидентов информационной безопасности. Помимо своего основного предназначения – предотвращения утечек информации – DLP-системы применимы и для решения целого ряда других задач, в том числе связанных с контролем действий персонала, например:

– контроль использования рабочего времени и ресурсов компании ее сотрудниками;

– мониторинг общения сотрудников с целью выявления разного рода интриг и других подобных явлений, которые могут серьезно осложнить деятельность организации;

– отслеживание реакции сотрудников на нововведения руководства;

– контроль соответствия действий сотрудников требованиям используемых политик безопасности и др.

Все DLP-системы можно разделить по ряду признаков на несколько основных классов. По способности блокирования информации, опознанной как конфиденциальная, выделяют системы с активным и пассивным контролем действий пользователя: первые умеют блокировать передаваемую информацию, вторые, соответственно, такой способностью не обладают. Первые системы гораздо лучше борются со случайными утечками данных, но при этом способны допустить непредвиденную остановку бизнес-процессов организации, вторые же безопасны для бизнес-процессов, но подходят только для борьбы с систематическими утечками. Еще одна классификация DLP-систем проводится по их сетевой архитектуре. Шлюзовые DLP работают на промежуточных серверах, в то время как хостовые используют агенты, работающие непосредственно на рабочих станциях сотрудников. Сегодня наиболее распространенным вариантом является совместное использование шлюзовых и хостовых компонентов.

Библиотека БГУИР

В настоящее время основными игроками мирового рынка DLP-систем являются компании, которые широко известны благодаря другим своими продуктам, предназначенным для обеспечения информационной безопасности. Это прежде всего Symantec, McAffee, TrendMicro, WebSense. Общий объем мирового рынка DLP-решений в 2014 г. оценивался более чем в 400 млн долларов, что, с одной стороны, совсем немного по сравнению с рынком, например, антивирусного программного обеспечения. С другой стороны, данная цифра свидетельствует о неплохих темпах роста рынка DLP-систем: еще в 2009 г. он оценивался суммой немногим более 200 млн долларов. В русле мировой тенденции следуют и рынки отдельных стран. Сегодня на российском рынке DLP-систем присутствуют как указанные выше известные мировые вендоры, так и отечественные производители – InfoWatch, «Инфосистемы Джет», SearchInform, SecureIT и др. Общий объем российского рынка DLP оценивается в 12–15 млн долларов, и растет он при этом теми же темпами, что и мировой.

Тем не менее имеется и ряд факторов, препятствующих повсеместному распространению подобных систем. Главными из них являются два: во-первых, высокая стоимость DLP-систем делает их доступными далеко не всем (как правило, лишь достаточно крупным и прибыльным компаниям), а во-вторых, их внедрение и использование требуют высокой квалификации персонала и немалых трудозатрат. Указанные обстоятельства могут с особенной силой проявиться в период ухудшения экономической ситуации в стране, однако вряд ли они способны полностью нивелировать очевидные выгоды использования DLP-систем в качестве комплексного эффективного инструмента для защиты конфиденциальной информации в организации.

По мнению экспертов, одной из основных современных тенденций в мире информационной безопасности является переход от «заплаточных» систем, состоящих из компонентов от различных производителей (каждый из них решает свою задачу), к единым интегрированным программным комплексам. Причина подобного перехода очевидна: комплексные интегрированные системы избавляют специалистов по информационной безопасности от необходимости решать проблемы совместимости различных компонентов «заплаточной» системы между собой, позволяют легко изменять настройки для больших массивов клиентских рабочих станций, помогают избегать трудностей при переносе данных из одного компонента единой интегрированной системы в другой.

Еще одной важной тенденцией развития DLP-систем является постепенный переход к модульным структурам, дающим возможность заказчику самостоятельно выбирать те компоненты системы, которые ему необходимы (например, если на уровне операционной системы отключена поддержка внешних устройств, то нет необходимости доплачивать за возможность их контроля средствами DLP-системы). Важную роль в развитии DLP-систем будет оказывать и отраслевая специфика – можно ожидать появление специальных версий известных систем, адаптированных к работе банковской сферы, для государственных органов, для производственных предприятий и т. д.

Библиотека БГУИР

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. DLP системы [Электронный ресурс] / Leta IT Company. – Режим доступа: http://www.leta.ru/library/analytics/inside-015/inside-015.html. – Дата доступа: 10.11.2019.

2. SearchInform AlertCenter [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/full-text-search-information-security-product-alerts-setting.html. – Дата доступа: 10.11.2019.

3. SearchInform DataCenter [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/full-text-search-information-security-product-datacenter.html. – Дата доступа: 10.11.2019.

4. SearchInform EndpointSniffer [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/full-text-search-information-security-product-endpoint-sniffer.html. – Дата доступа: 10.11.2019.

5. SearchInform NetworkSniffer [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/full-text-search-information-security-product-network-sniffer.html. – Дата доступа: 10.11.2019.

6. SearchInform ReportCenter [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/reportCenter.html. – Дата доступа: 10.11.2019.

7. Symantec DLP – первая в мире DLP-система на русском языке среди лидеров рынка [Электронный ресурс] / Symantec Corporation. – Режим доступа: http://www.symantec.com/ru/ru/about/news/release/article.jsp?prid=20100901_01. – Дата доступа: 10.11.2019.

8. Барабанов, А. В. Формирование требований к сертификационным испытаниям DLP-систем по требованиям безопасности информации / А. В. Барабанов, М. И. Гришин, А. С. Марков // Вестн. МГТУ им. Н. Э. Баумана. Электронное научно-техническое издание. – 2013. – № 2 (14). – С. 1–8.

9. Васильев, В. DLP-системы на этапе перевода ИТ на облачную платформу / В. Васильев // PC Week Review: ИТ-безопасность. – 2011. – № 3. – С. 14–16.

10. Индексация рабочих станций [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/full-text-search-information-security-product-indexing-connectors.html. – Дата доступа: 10.11.2019.

11. Контур информационной безопасности SearchInform [Электронный ресурс] / SearchInform. – Режим доступа: http://searchinform.ru/main/full-text-search-information-security-product.html. – Дата доступа: 10.11.2019.

12. Кузнецов, А. А. Защита деловой информации / А. А. Кузнецов. – М. : Экзамен, 2008. – 239 с.

13. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2011 г. / В. А. Матвеев [и др.] // Вестн. МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». Спецвыпуск «Технические средства и системы защиты информации». – 2011. – С. 3–6.

14. Морозова, Н. С. Проблемы современных систем предотвращения утечек данных с конечных точек сети / Н. С. Морозова // Безопасность информационных технологий. – 2011. – № 4. – С. 138–143.

15. Окулесский, В. Безопасность под флагом DLP [Электронный ресурс] / В. Окулесский. – Режим доступа: http://bis-expert.ru/articles/44149. – Дата доступа:10.11.2019.

16. Основные игроки российского рынка DLP [Электронный ресурс] / Банкир.Ру. – Режим доступа: http://bis-expert.ru/articles/44149. – Дата доступа: 10.11.2019.

17. Пшехотская, Е. Лингвистика в DLP-системах [Электронный ресурс] / Е. Пшехотская. – Режим доступа: http://bis-expert.ru/articles/42696. – Дата доступа: 10.11.2019.

18. Скиба, В. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с.

19. Федоров, Н. Возможные метрики ИБ при выборе и использовании DLP-систем / Н. Федоров // PC Week Review: ИТ-безопасность. – 2011. – № 3. – С. 16.

20. Федотов, Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М.: Юридический Мир, 2007. – 432 с.

21. Хайретдинов, Р. Как работают DLP-системы? / Р. Хайретдинов // Хакер. – 2011. – № 3. – С. 18–121.

22. Харченко, Д. DLP – что это значит? [Электронный ресурс] / Д. Харченко // PCWEEK live: корпоративные информационные технологии и решения. – Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=109716. – Дата доступа: 10.11.2019.

23. Шабанов, И. Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2009–2011 [Электронный ресурс] / И. Шабанов, К. Ренселаева // Anti-Malware: информационно-аналитический центр. – Режим доступа: http://www.anti-malware.ru/russian_dlp_market_2009_2011. – Дата доступа: 10.11.2019.

24. Шабанов, И. Сравнение систем защиты от утечек (DLP) 2014. Ч. 1 [Электронный ресурс] / И. Шабанов. – Режим доступа: http://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1. – Дата доступа: 10.11.2019.

25. Шабанов, И. Сравнение систем защиты от утечек (DLP) 2014. Ч. 2 [Электронный ресурс] / И. Шабанов. – Режим доступа: http://www.anti-malware.ru/comparisons/data_leak_protection_2014_part2. – Дата доступа: 10.11.2019.

26. Шихов, Е. Обзор DLP-систем на мировом и российском рынке [Электронный ресурс] / Е. Шихов. – Режим доступа: http://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014. – Дата доступа: 10.11.2019.

27. Юридическое, техническое и информационно-аналитическое обеспечение оперативно-розыскной деятельности : учеб. пособие / под ред. А. Н. Халикова. – М. : Юрлитинформ, 2010. – 472 с.

Библиотека БГУИР

Библиотека БГУИР

Св. план 2020, поз. 34

Учебное издание

Борботько Тимофей Валентинович
Бойправ Ольга Владимировна
Морозов Виктор Егорович
Дрозд Алексей Валерьевич

СИСТЕМА ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ДАННЫХ «КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM»

ПОСОБИЕ

Редактор *М. А. Зайцева*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *Е. Г. Бабичева*

Подписано в печать 17.02.2021. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс». Отпечатано на ризографе. Усл. печ. л. 16,62. Уч.-изд. л. 17,7. Тираж 30 экз. Заказ 178.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники». Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий №1/238 от 24.03.2014, №2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск

Библиотека БГУИР