ПРОГРАММНЫЙ КОМПЛЕКС

«Серчинформ ДЛП»

Описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения, в том числе
устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения,
совершенствование программного обеспечения, а также информация о персонале, необходимом для обеспечения такой поддержки

на 21 листе

Оглавление

1 Описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения 3
2 Эксплуатация ПО 4
3 Сопровождение (регламентные и профилактические работы)....5
4 Совершенствование (обновление) ПО....6
4.1 Обновление серверной части ПО 6
4.2 Получение обновлений клиентскими рабочими станциями с серверов....6
4.3 Порядок установки обновлений программного обеспечения 6
4.4 Периодичность выхода новых версий ПО 7
5 Устранение неисправностей в ходе эксплуатации ПО 8
5.1 Типовые неисправности и способы их решения....8
5.1.1 Проблемы в работе сервера NetworkController 8
5.1.2 Проблемы в работе сервера EndpointController....11
5.1.3 Проблемы в работе сервера индексации Search Server....14
5.1.4 Проблемы в работе клиентского приложения....15
5.1.5 Проблемы в работе модуля администрирования DataCenter 17
5.2 Нетиповые неисправности 19
6 Персонал, необходимый для обеспечения поддержки ПО....20
6.1 Обязанности сетевого администратора 20
6.2 Обязанности администратора аппаратного обеспечения 20
6.3 Обязанности администратора системы (администратора ПО) 20
6.4 Обязанности офицера безопасности 21

1 Описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения

Перечень процессов, обеспечивающих поддержание жизненного цикла программного обеспечения на этапе эксплуатации в инфраструктуре конечного пользователя:

1. Эксплуатация;
2. Сопровождение (регламентные и профилактические работы);
3. Совершенствование (обновление, модификация);
4. Устранение неисправностей (восстановление) программного обеспечения в ходе эксплуатации.

Схема процессов представлена на рисунке 1.1.

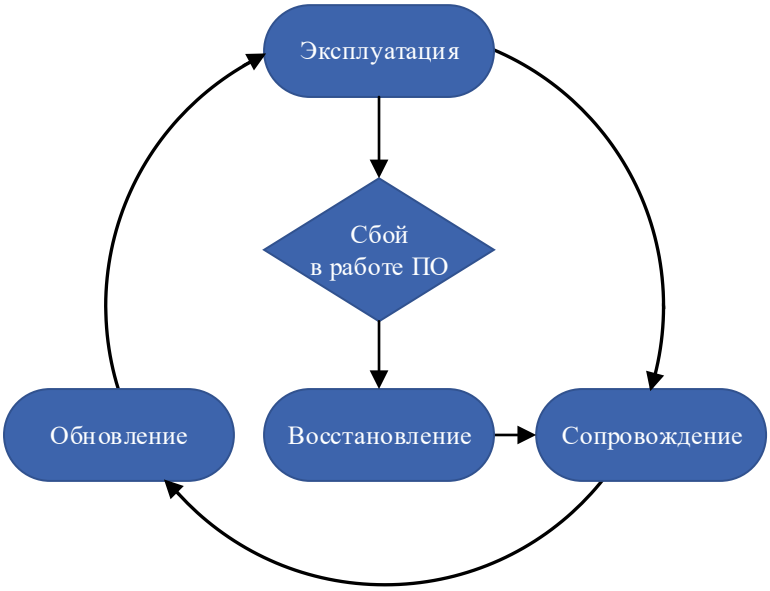

Рисунок 1.1. Схема процессов

2 Эксплуатация ПО

Эксплуатация ПО осуществляется в соответствии со следующими документами:

- Серчинформ ДЛП. «Руководство администратора»;
- Серчинформ ДЛП. «Руководство пользователя».

3 Сопровождение (регламентные и профилактические работы)

Порядок состав и периодичность проведения профилактических работ приведены в таблице.

Вид регламента	Длительность	Основные операции	Исполнитель
Ежемесячный	1 ч.	Контроль целостности БД	Администратор Системы
Ежемесячный	1 ч.	Анализ истории работы заданий по расписанию Отслеживание заданий с чрезмерной продолжительностью	Администратор Системы
Ежедневно	15 мин.	Контроль автоматического выполнения резервного копирования	Администратор Системы
По требованию	30 мин.	Установка обновлений	Администратор Системы
Ежедневный	30 мин.	Анализ журнала регистрации событий безопасности	Администратор Системы
Ежедневно	15 мин.	Проверка состояния ОС сервера Системы	Администратор Системы
Ежедневно	15 мин.	Проверка работоспособности компонентов ПО штатными средствами	Администратор Системы
Ежедневно	15 мин.	Проверка функций перехвата	Администратор Системы
При необходимости	15 мин.	Проверка доступности серверов Системы штатными средствами	Администратор Системы
При необходимости	15 мин.	Проверка состояния СУБД	Администратор Системы
При необходимости	15 мин.	Проверка работы механизма системных уведомлений	Администратор Системы
При необходимости	15 мин.	Проверка синхронизации каталога домена	Администратор Системы
При необходимости	15 мин.	Проверка лицензии Системы	Администратор Системы

4 Совершенствование (обновление) ПО

4.1 Обновление серверной части ПО

Обновление версий компонентов Серчинформ ДЛП производится путем установки поверх существующей версии обновляемого продукта. Удаление старой версии не требуется.

Перед установкой новой версии остановите службу сервера обновляемого компонента, закройте консоль администрирования и клиентскую консоль. Если на сервере установлены и другие компоненты Серчинформ ДЛП, остановите все их службы и закройте все их окна!

При установке новой версии будут по умолчанию выбраны те же компоненты, что и при установке предыдущей версии ПО, и будут сохранены все существующие настройки, индексы и лицензия. Не изменяйте реестр операционной системы!

Дополнительную настройку сервера производить не требуется.

4.2 Получение обновлений клиентскими рабочими станциями с серверов

Получение обновлений клиентскими рабочими станциями производится автоматически с сервера. Периодичность получения обновлений – по мере необходимости, за исключением критических случаев.

Инициация рассылки обновлений производится Администратором Системы.

В случае неуспешной установки будет сформировано сообщение с ошибкой. В этом случае Администратор Системы должен устранить причины возникновения ошибки и запустить процесс обновления еще раз. Если ошибка относится к функциям Системы, Администратор Системы должен проинформировать Разработчика Системы по телефону или электронной почте. В свою очередь, после регистрации инцидента сотрудники Разработчика Системы информируют Администратора Системы о действиях по устранению ошибки.

4.3 Порядок установки обновлений программного обеспечения

Установка обновлений производится Администратором Системы. Периодичность установки обновлений – по мере необходимости, за исключением критических случаев.

Новые версии ПО Системы передает Разработчик Системы.

Инициация установки обновлений производится Администратором Системы.

Проведение работ на серверах осуществляется по предварительно согласованному со всеми участниками плану. Установка обновлений серверной части Системы производится путем установки соответствующих компонент в соответствии с описанием данных процессов в руководстве администратора.

Перед проведением любых изменений с серверными компонентами Системы необходимо произвести резервное копирование изменяемого компонента или сервера, где он находится. После проведения изменений так же необходимо провести резервное копирование и убедиться, что оно работает. В обратном случае производится откат всех произведенных изменений.

Установка обновлений клиентской части Системы производится путем установки соответствующих компонент в соответствии с описанием данных процессов в руководстве администратора.

Учет обновлений производится Администратором Системы путем записи произведенных изменений в Журнал обновлений системы. Производится запись следующих

пунктов:

- Дата и время обновления.
- Перечень обновленных компонентов.
- Версия обновленных компонентов.
- Причина произведенного обновления.
- Фамилия и имя сотрудника, производившего обновление.

4.4 Периодичность выхода новых версий ПО

Периодичность выхода новых версий ПО в соответствии с внутренним планом составляет не менее 2 раз в год, однако частота выхода новых версий ПО может увеличиваться в зависимости от ряда условий:

- Пользователи массово обращаются в техническую поддержку с одинаковой ошибкой;
- Разработчик стороннего ПО внес изменения, которые привели к неработоспособности одного или нескольких модулей/компонентов ПО;
- Внесены изменения в нормативную документацию, касающуюся функционала и использования ПО.

Информация о новых версиях ПО рассылается пользователям ПО по электронной почте.

5 Устранение неисправностей в ходе эксплуатации ПО

5.1 Типовые неисправности и способы их решения

5.1.1 Проблемы в работе сервера NetworkController

5.1.1.1 Не отображаются имена пользователей

Симптом: Вместо доменных имен, в выдаче клиента отображено значение <Unknown>. Это означает, что не настроено или некорректно настроено взаимодействие системы с контроллером домена (см. Рисунок 5.1).

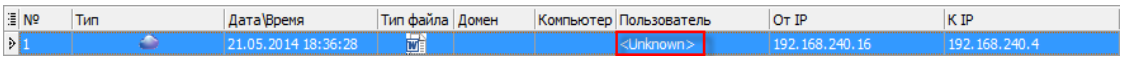

Рисунок 5.1

Возможные причины:

- недостаточные права сервиса перехвата;
- отключена индексация атрибутов документов;
- закрыты порты взаимодействия с контроллером домена.

5.1.1.2 Недостаточные права сервиса перехвата

Сервис перехвата должен быть запущен под учетной записью, включенной в доменные политики «Создание журналов безопасности» (Generate security audits) и «Управление аудитом и журналом безопасности» (Manage auditing and security log).

Процедура настройки подробно изложена в п. 6.6.6 Руководства Администратора.

5.1.1.3 Закрыты порты взаимодействия с контроллером домена

Закрыты порты, используемые для подключения к журналу событий безопасности контроллера домена. Порты должны быть открыты.

NetworkController делает запрос, чтобы узнать имя контроллера домена. Это соединение происходит по протоколу CLDAP. Локальные порты этого соединения находятся в диапазоне 19**, удаленный порт (на контроллере домена) – 389. Данные порты, скорее всего, будут открыты по умолчанию, иначе компьютер не сможет войти в домен.

После того, как NetworkController получает имя контроллера домена, он подключается к журналу и начинает получать из него данные. Соединение происходит по протоколу SMB. Локальный порт соединения – 2002, удаленный порт (на контроллере домена) – 445.

5.1.1.4 Сообщения не перехватываются

Причина: Использование нестандартных портов.

По умолчанию NetworkController перехватывает трафик, ходящий по стандартным портам, перечисленным в Таблица 1.

Таблица 1 – Список используемых протоколами портов по умолчанию

Протоколы	Порты по умолчанию
Web mail	80
IMAP	143
MAPI	1118[1]

[1] Значение по умолчанию. Если на сервере Microsoft Exchange явным образом задан один порт, нужно прослушивать только его. Если явной привязки протокола MAPI к портам нет, нужно прослушивать весь доступный диапазон портов.

Протоколы	Порты по умолчанию
POP3	110
SMTP	25
NNTP (NNTPS)	119 (563)
HTTP POST	80
ICQ	443
MMP	2041
XMPP	5222
SIP	5060
HTTP IM	80
FTP	21

Решение: Для корректной работы перхвата проверьте, настроены ли нестандартные номера портов. Например, для передачи SMTP-трафика обычно используется порт 25, но может использоваться и порт 2525, а для протокола MAPI порты могут выбираться случайным образом, если на сервере Microsoft Exchange не задано жесткой привязки протокола к портам.

Для настройки привязок по портам, в группе «Сетевой перехват» выделите узел «Протоколы» и перейдите на вкладку «Настройки портов» (см. Рисунок 5.2).

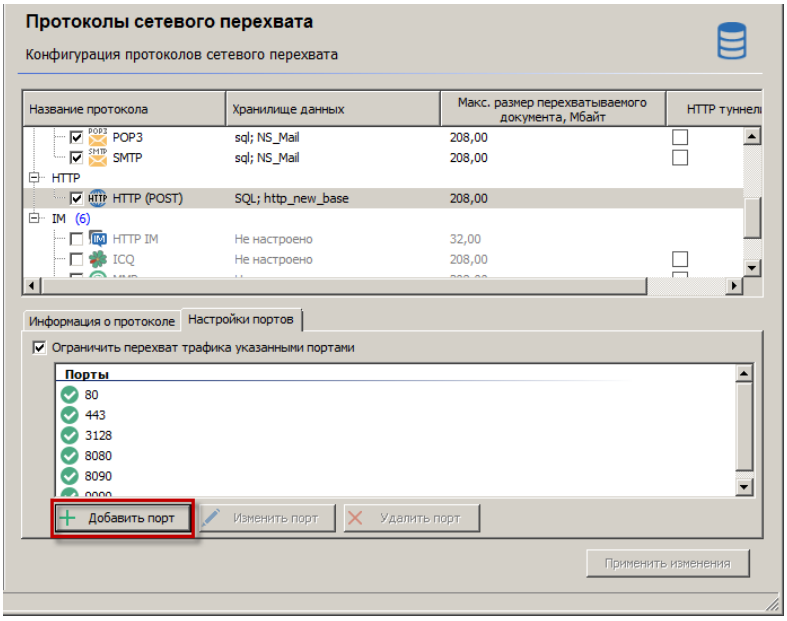

Рисунок 5.2

Фильтры по портам могут быть разрешающие или запрещающие. Фильтр может включать один порт (см. Рисунок 5.3) или диапазон портов (см. Рисунок 5.4).

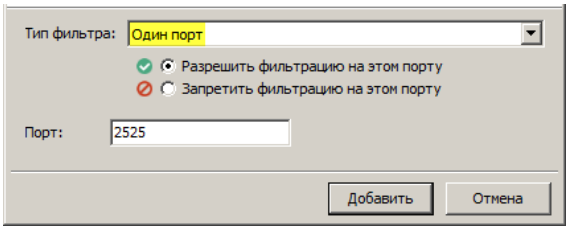

Рисунок 5.3

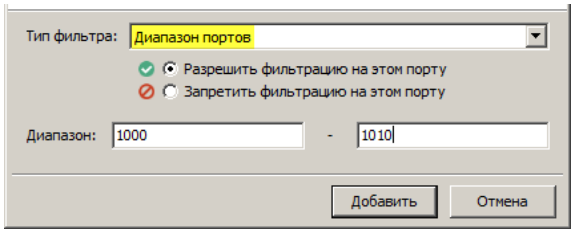

Рисунок 5.4

5.1.1.5 Неполный перехват данных

При подозрении на потерю пакетов рекомендуется:

- убедиться, что в настройках сетевых адаптеров отключены все «offload»-параметры);
- снять трафик с помощью программы-анализатора Wireshark и сравнить его с трафиком, перехваченным сервером NetworkController.

Wireshark – один из лучших анализаторов сетевого трафика, используемый сетевыми администраторами для выявления проблем в сети. Программа распространяется бесплатно и может быть загружена с www.wireshark.org.

Если настройки адаптеров соответствуют требованиям, а трафик Wireshark и NetworkController отличается количеством перехваченных документов, существует возможность смены библиотеки перехвата с Packet Sniffer SDK (pssdk.dll) на WinPcap (wpcap.dll). Однако данный механизм перехвата рекомендуется использовать лишь в крайнем случае, поскольку его работа существенно медленнее стандартного.

Для смены библиотеки перехвата откройте конфигурационный файл **sinssvc.xml**, расположенный по адресу: %ProgramFiles%\SearchInform\SearchInform NetworkController\SearchInform NetworkController Server\ .

Внутри корневого тега <sinssvc> пропишите строку (см. Рисунок 5.5)**:**

<sniffer>wpcap</sniffer>.

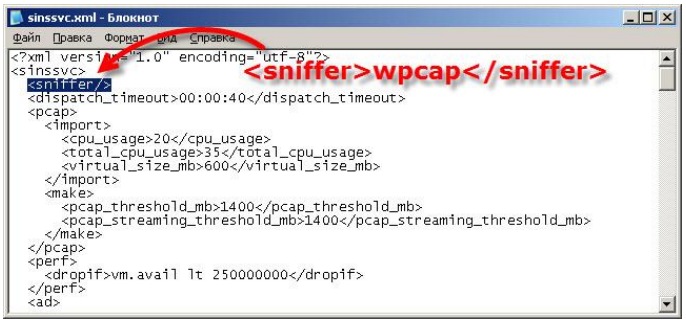

Рисунок 5.5

Сохраните измененный файл.

5.1.1.6 Не запускается служба перехвата

Причина: Изменение доменных политик и отмена права входа в качестве службы для пользователя домена, под учетной записью которого запускается сервис NetworkController.

Решение: см. Руководство Администратора, раздел «Настройка прав входа в качестве службы».

5.1.2 Проблемы в работе сервера EndpointController

5.1.2.1 Агенты не устанавливаются или не обновляются

Симптом 1: После выбора рабочих станций и нажатия кнопки «Применить» не отображаются маркеры «✔».

Симптом 2: Не происходит обновления версий агентов или версии агентов не отображаются (см. Рисунок 5.6).

Без установленных агентов перехват невозможен!

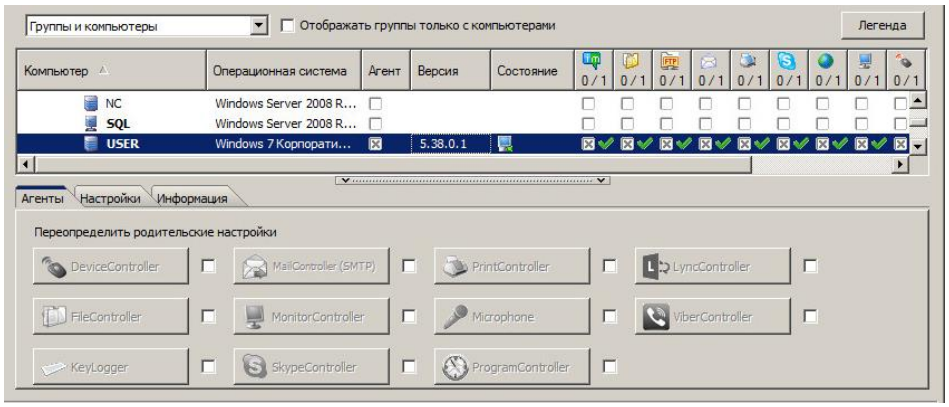

Рисунок 5.6

Журнал удачных и неудачных попыток установки агентов на рабочие станции пользователей можно просмотреть на вкладке «Текущая активность» (см. Рисунок 5.7).

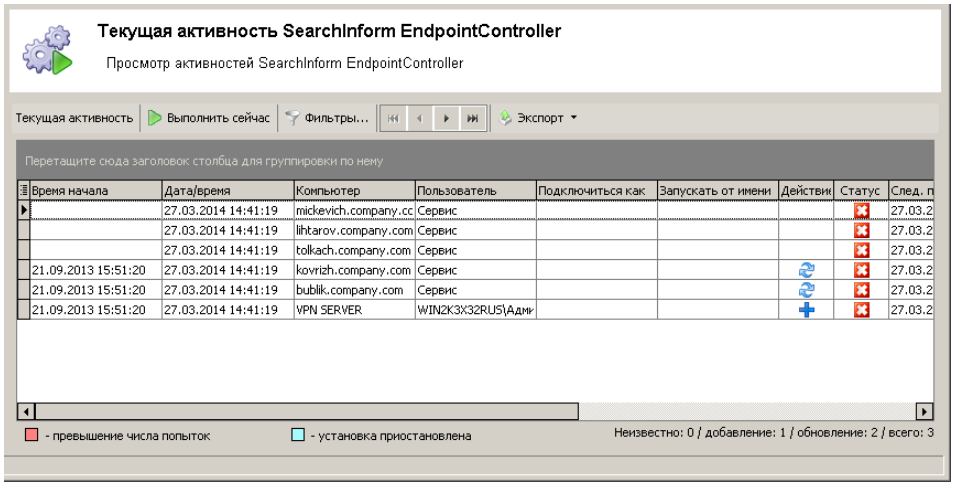

Рисунок 5.7

Журнал текущего состояния установок агентов включает в себя следующие параметры:

- **Время начала** – дата и время начала первой попытки установить/удалить/ обновить агент на рабочей станции;
- **Дата/время** – дата и время начала текущей попытки установить/удалить/ обновить агент на рабочую станцию;

- **Компьютер** – имя компьютера, на который устанавливался или был установлен агент;
- **Пользователь** – имя пользователя, инициировавшего активность;
- **Подключиться как** – учетная запись, от которой производится установка агента (при включенной опции «Подключаться как»);
- **Запускать от имени** – учетная запись, от которой производится запуск агента (при включенной опции «Запускать от имени»);
- **Действие** – значок, указывающий на действие, которое производится с агентом;
- **Статус** – значок, отображающий статус сообщения;
- **След. попытка** – дата и время следующей попытки установить/удалить/ обновить агент;
- **Попыток** – число попыток, предпринятых для установки/удаления/обновления агента;
- **Сообщение** – пояснение о выполнении/невыполнении определенного действия над агентом;
- **Описание** – описание рабочей станции, заданное в Active Directory, либо на вкладке «Сетевое окружение»;
- **Комментарии** – пользовательский комментарий к определенной рабочей станции, задаваемый на вкладке «Сетевое окружение».

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,
-  - обновление со стороны агента.

Возможные сочетания «проблема-решение»:

- агенты не устанавливаются – отмена запрета на установку;
- агенты не устанавливаются – установка вручную;
- агенты установлены, но не передают данные – запуск служб под другой учетной записью.

5.1.2.2 Агенты не устанавливаются – отмена запрета на установку

Симптом: Агенты не устанавливаются.

Причина: Новые агенты не будут устанавливаться, если в отношении их установки действует запретительный режим (по умолчанию действует разрешительный режим на установку агентов) (см. Рисунок 5.8).

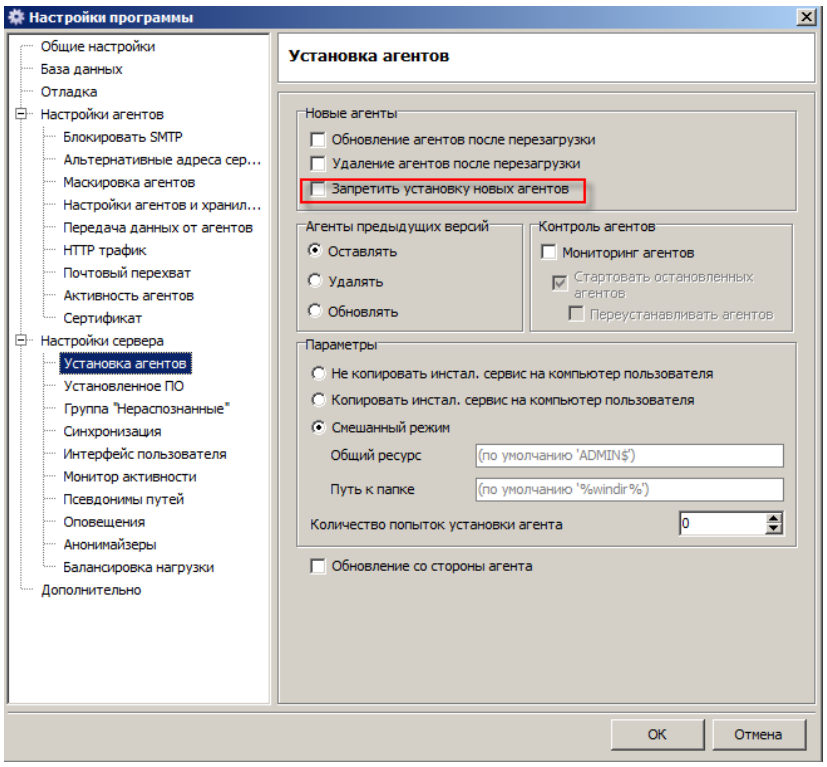

Рисунок 5.8

Решение: Перейдите в настройки EndpointController и выберите вкладку «Установка агентов». Снимите флажок «Запретить установку новых агентов» и щелкните «OK».

5.1.2.3 Агенты не устанавливаются – установка вручную

Симптом: Агенты не устанавливаются, протоколы не включаются.

Причина: Служба сервера EndpointController имеет недостаточно прав для установки агента, установке соединения мешает брандмауэр и др.

Решение: Установка агентов вручную.

Подробное описание решения проблемы приводится в Руководстве Администратора.

5.1.2.4 Агенты установлены, но не передают данные – запуск служб под другой учетной записью

Симптом 1: Агенты установлены, серверные службы работают, но индекс остается пустым при обновлении (проиндексировано 0 документов).

Симптом 2: Агенты установлены, службы работают, перехват был, но исчез, или не обновляются версии агентов.

Наиболее вероятная причина: Недостаточно прав у служб EndpointController (например, изменились доменные политики).

Решение: Настройте вход служб SIAMSControlSvc и SIMHSvc под учетной записью с правами администратора домена.

Сочетанием клавиш **Win+R** откройте окно «Выполнить», введите команду **services.msc**. Будет открыта оснастка «Службы», отображающая список служб и их состояние. Сервер EndpointController использует службы SearchInform EndpointController Agents Control (SIAMSControlSvc.exe), SearchInform EndpointController Agents Check (SIMHAgentCheck.exe) и SearchInform EndpointController (SIMHSvc.exe) (см. Рисунок 5.9).

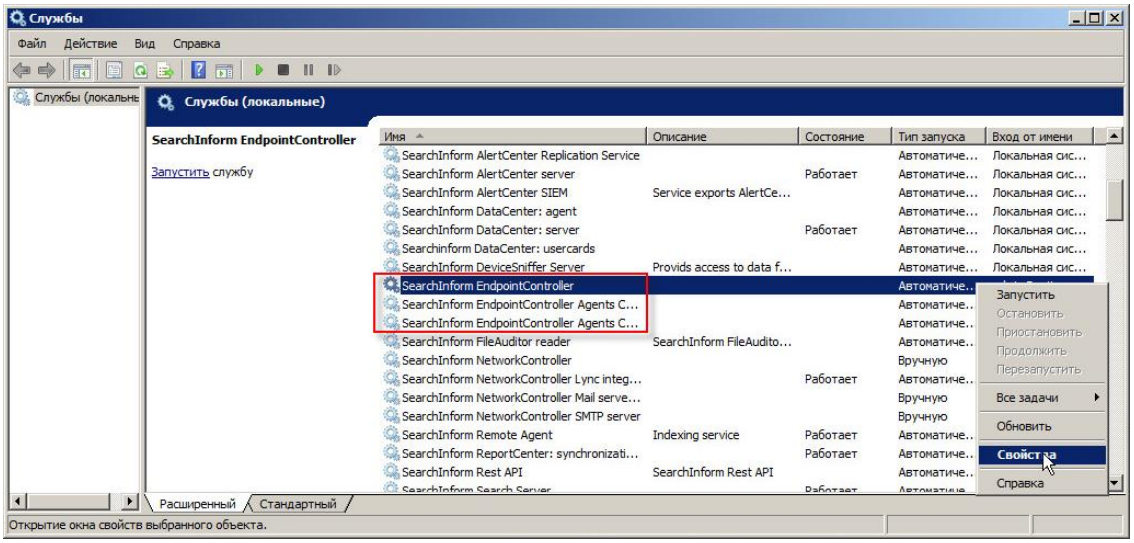

Рисунок 5.9

Откройте свойства служб на вкладке «Вход в систему». Выберите опцию «С учетной записью» и введите параметры учетной записи пользователя с правами администратора домена (см. Рисунок 5.10).

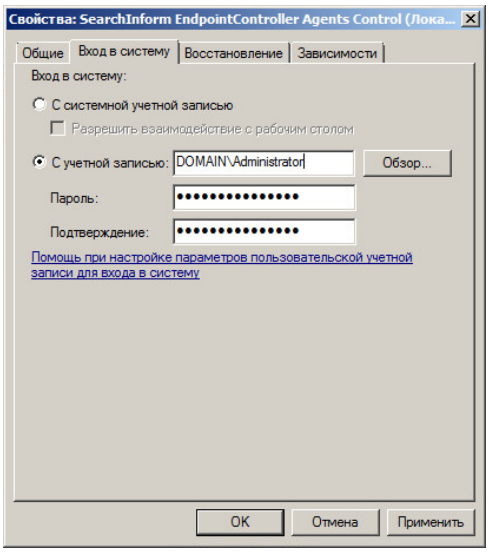

Рисунок 5.10

После изменения прав входа перезапустите службы.

5.1.3 Проблемы в работе сервера индексации Search Server

5.1.3.1 Невозможно выполнить индексацию

Симптом: При запуске индексации отображается сообщение о невозможности произвести индексацию.

Причина: Сохранение перехваченных по разным каналам коммуникации документов в одной базе данных.

Решение: Пересоздайте базу данных. Для каждого канала передачи данных создается отдельный индекс и соответственно – отдельная база данных. Сохранение перехваченных по разным каналам связи данных в одну базу приводит к сбоям в работе сервера индексации.

5.1.4 Проблемы в работе клиентского приложения

5.1.4.1 Нехватка памяти

Симптом: При нехватке памяти, клиент может отображать сообщение о динамической ошибке (run-time error).

Причина: Такая ошибка вызвана нехваткой памяти на построение списка документов.

Решение: Для разрешения проблемы уменьшите число документов в выдаче клиента.

Откройте настройки AnalyticConsole. На вкладке «Результаты поиска» ограничьте количество выдаваемых в консоли результатов поиска (см. Рисунок 5.11).

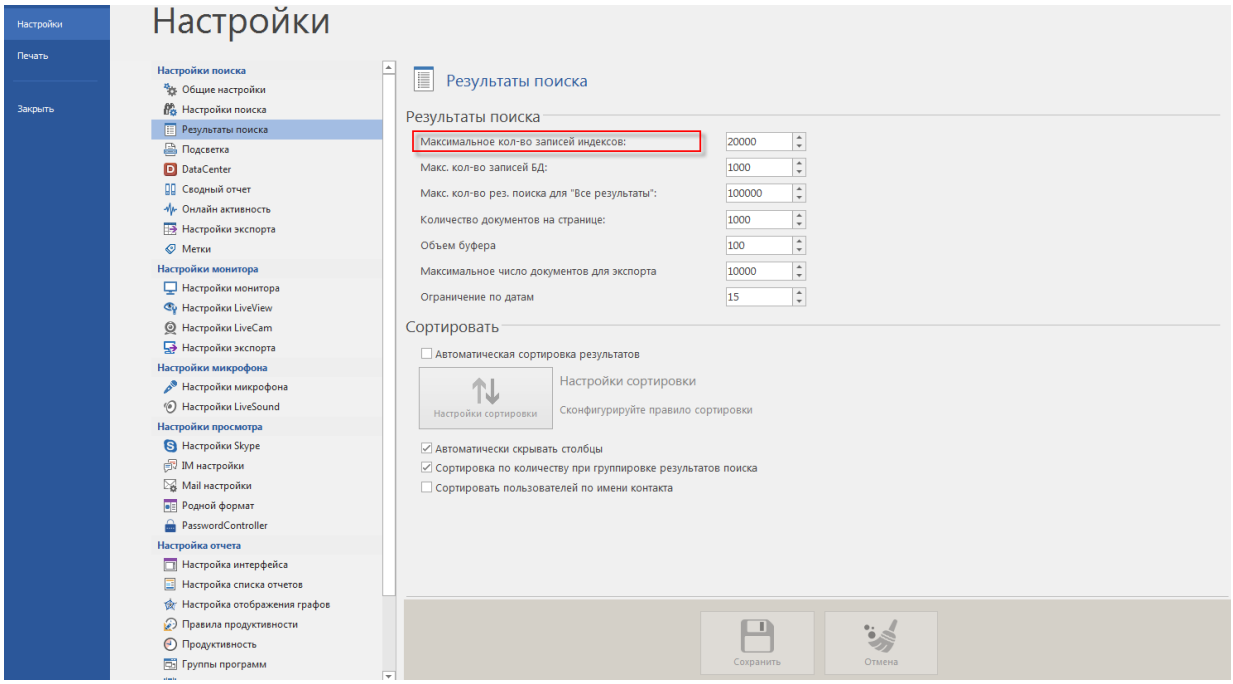

Рисунок 5.11

5.1.4.2 Проблемы с кодировкой при отображении сообщений в клиенте

Симптом: Клиент отображает сообщения в некорректной кодировке.

Решение: Выберите вручную верную кодировку из контекстного меню окна предпросмотра (см. Рисунок 5.12).

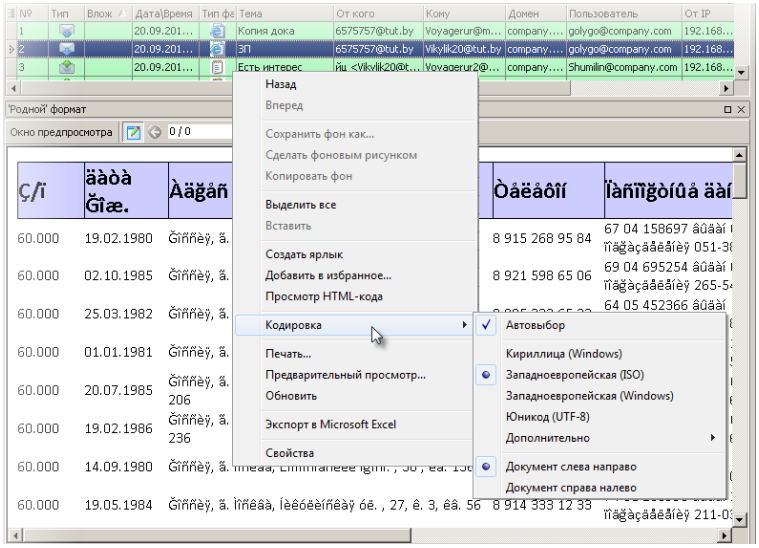

Рисунок 5.12

5.1.4.3 Переходы по отчетам не производятся

Симптом: В окне просмотра отчетов не производятся переходы, правая клавиша не вызывает контекстное меню.

Причина: Автопереходы и контекстное меню отключены в настройках клиента ReportCenter.

Решение: Установите флажки «Разрешить автопереходы …» и выберите опцию переходов по диаграммам «По правой кнопке мыши» (см. Рисунок 5.13).

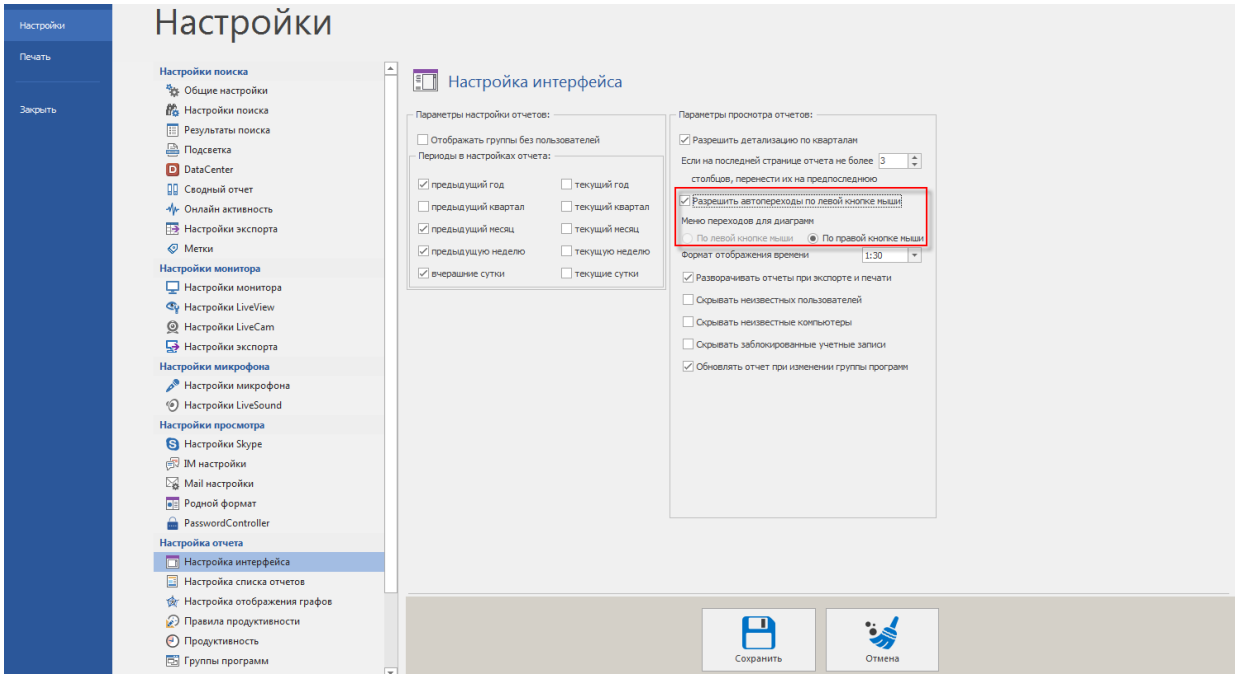

Рисунок 5.13

5.1.4.4 Отображаются пустые отчеты

Симптом: отображаются пустые отчеты.

Причина: Не подключены источники данных или сервер ReportCenter не синхронизирован с ними.

Решение: Подключите источники данных и/или произведите синхронизацию.

5.1.4.5 Статистика не обновляется

Симптом: статистика не обновляется.

Причина: Сервер и AnalyticConsole подключены к разным базам.

Решение: Произведите подключение сервера ReportCenter и AnalyticConsole к одной базе.

5.1.5 Проблемы в работе модуля администрирования DataCenter

5.1.5.1 Контролируемые компоненты не отображаются или отображаются некорректно

Симптом: Не отображаются серверы контролируемых компонентов, на которые были установлены агенты DataCenter (см. Рисунок 5.14).

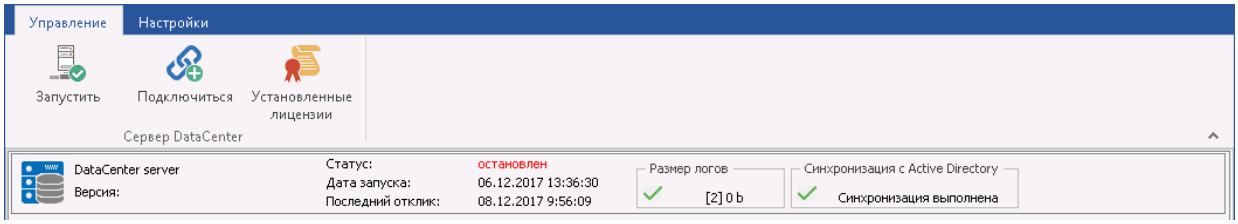

Рисунок 5.14

Причина: Задан неверный путь от агента к серверу DataCenter.

Решение: Произведите повторную установку агентов DataCenter. При этом укажите правильный путь к серверу DataCenter.

5.1.5.2 Уведомления не доставляются

Симптом: Настроена доставка уведомлений, но уведомления не доставляются.

Причина 1: Неправильные настройки подключения к серверу SMTP.

Причина 2: Неверный адрес получателя.

Причина 3: Неверный адрес отправителя.

Решение: Проверьте настройки подключения к SMTP-серверу.

Щелкните кнопку «Почтовые уведомления», расположенную на панели «Настройки». Нажмите кнопку «Проверить соединение» (см. Рисунок 5.15).

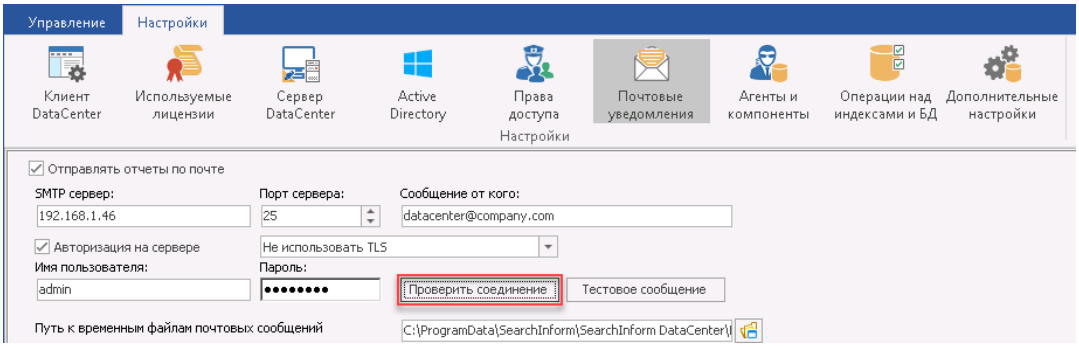

Рисунок 5.15

Будет отображено одно из следующих сообщений:

- «Не удалось установить соединение» - неверно указан SMTP-сервер, SMTP-порт или отправитель. Укажите верные настройки.

– «Не удалось пройти аутентификацию» - неверные настройки аутентификации. Установите флажок «Аутентификация на сервере», введите корректные имя учетной записи и пароль.

После настройки кликните кнопку «Проверить соединение. Если введены верные настройки, будет отображено сообщение «Соединение успешно установлено!».

Для отправки тестового сообщения на электронный адрес аудитора безопасности используется кнопка «Тестовое сообщение».

Если проблема заключалась в неверном адресе отправителя или получателя, очистите папку «MailTemp\», расположенную в папке с логами DataCenter (см. Рисунок 5.16).

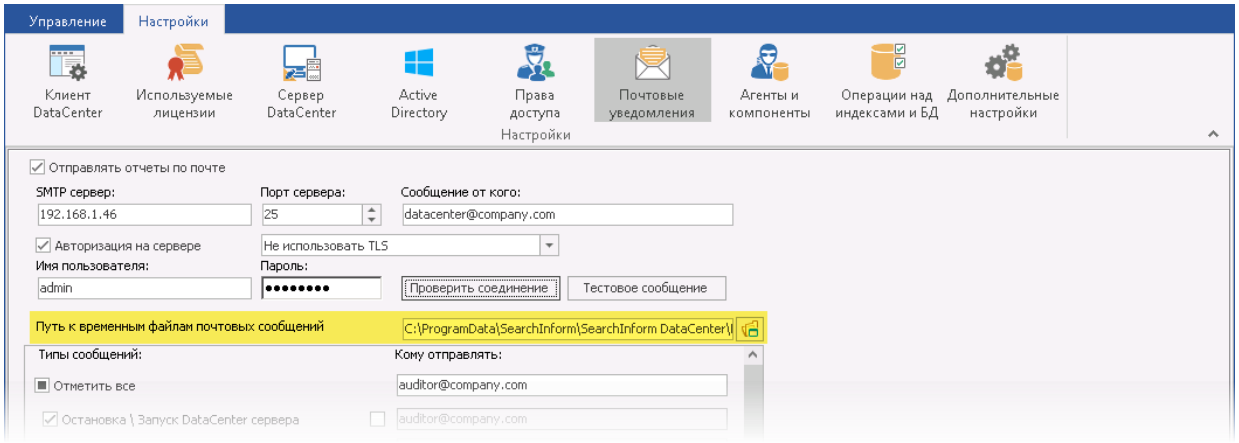

Рисунок 5.16

5.1.5.3 Сервер в списке выделен красным цветом

Выделение имени сервера красным цветом свидетельствует о наличии проблем в работе его компонентов. Например, если не запущен какой-либо из установленных на сервере продуктов или отсутствует доступ к базе перехвата, или возникли ошибки при разбиении индексов и БД. Для обнаружения источника ошибки разверните список компонентов сервера, имя которого подсвечено красным, нажав  . Компонент с критической ошибкой также выделен в списке красным цветом.

Симптом: Имя сервера выделено в списке красным цветом.

Причина 1: Ошибки при разбиении индекса или БД компонентов сервера.

Решение 1: Проверьте, не «загорелась» ли напротив компонента иконка  (Рисунок 5.17).

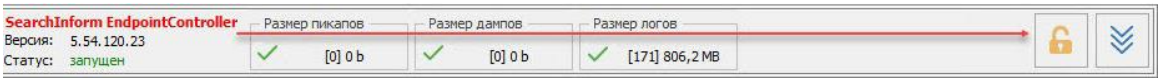

Рисунок 5.17

Данное обстоятельство означает, что произошла блокировка автоматических действий по продукту, требующая выяснения и устранения причины. При этом индексация данных будет происходить в штатном режиме, а автоматическое разбиение, удаление, принудительные запуск и перезапуск по данному модулю происходить не будут.

После устранения причины, вызвавшей неполадку, щелкните по иконке  , чтобы деактивировать блокировку. Значок приобретет монохромные цвета.

Если других ошибок нет, красный цвет названия компонента сменится обычным.

Причина 2: Доступ к базе данных отсутствует.

Решение 2: Наведите курсор мыши на компонент, подсвеченный красным цветом, и дождитесь отображения всплывающего окна, отображающего информацию по корректности доступа к индексам и БД.

Шаблон отображаемой сводки следующий:

протокол [<СУБД> полное_доменное_имя_компьютера; имя_БД]: статус

Обратите внимание на протоколы, перед которыми стоит символ «*****», отображающийся при *незаданных настройках БД*, *отсутствии индекса*, настроенного на данную БД по указанному протоколу, а также при *отключенном перехвате данных*.

Если Вы видите статус «*нет доступа*», это означает, что доступ к базе данных этого протокола отсутствует (база данных удалена, изменены настройки подключения к базе данных и пр.).

Если других ошибок нет, красный цвет названия компонента сменится обычным.

5.2 Нетиповые неисправности

При возникновении других неисправностей, конечный пользователь имеет право обратиться в службу технической поддержки (при наличии действующего договора на техническую поддержку) по следующим контактным данным:

- тел.: +7 (843) 206-07-43
- e-mail: sintegra-kaz@yandex.ru

Нетиповые неисправности могут быть устранены путем:

- Консультаций по их устранению;
- Устранения силами специалиста службы технической поддержки путем перенастройки параметров работы существующего ПО;
- Устранения внутренних ошибок ПО (ошибок в исходном коде) путем выпуска массового обновления ПО и предоставления новой/обновленной версии ПО.

В рамках технической поддержки также оказываются следующие услуги:

- Помощь в установке ПО, новых версий.
- Консультирование по настройке и эксплуатации консолей управления ПО.
- Консультирование по вопросам эксплуатации клиентских приложений ПО.
- Консультирование по вопросам анализа перехваченной информации.
- Предоставление информации по новым версиям.
- Консультирование по работе новых версий.
- Предоставление новых версии посредством отправки ссылок для скачивания по электронной почте.
- Помощь в проведении обновлений.
- Помощь при возникновении проблем в работе ПО.
- Выезд специалиста в случае невозможности решить проблемы в работе ПО удаленно.

6 Персонал, необходимый для обеспечения поддержки ПО

Для обслуживания ПО необходимо наличие персонала со следующими ролями:

1. Сетевой администратор;
2. Администратор аппаратного обеспечения;
3. Администратор ПО
4. Офицер безопасности.

Обслуживающий персонал должен обладать необходимой квалификацией и знаниями в объеме, достаточном для успешного выполнения своих задач. В зависимости от численности обслуживающего персонала указанные обязанности могут быть совмещены.

При выполнении своих задач обслуживающий персонал должен руководствоваться технической документацией, предоставленной Разработчиком Системы.

6.1 Обязанности сетевого администратора

В обязанности администратора сети входит сопровождение сетевых коммуникаций, а именно:

- Настройка локальной сети и обеспечение ее функционирования;
- Конфигурирование сетевых протоколов и портов;
- Обеспечение необходимого качества функционирования серверов сети, в том числе серверов Системы;
- Планирование и проведение работ по расширению сетевой структуры предприятия.

6.2 Обязанности администратора аппаратного обеспечения

В обязанности администратора аппаратного обеспечения входит:

- Выбор, установка и конфигурирование аппаратного обеспечения, рекомендуемого Разработчиком Системы;
- Настройка прокси- и почтовых серверов, свитча с функцией зеркалирования;
- Установка и настройка антивирусного ПО и файерволов.

6.3 Обязанности администратора системы (администратора ПО)

Администратор Системы отвечает за стабильность и безотказность работы ПО.

Обязанностями Администратора Системы являются:

- Создание и поддержание в актуальном состоянии пользовательских учётных записей, наделение их достаточными правами;
- Установка и настройка СУБД, резервное копирование баз данных, сохранение резервных копий; восстановление баз данных; архивирование информации;
- Развертывание и настройка Системы;
- Установка обновлений компонент Системы;
- Формирование ролей пользователей Системы и перечня их прав;
- Назначение ролей Системы офицерам безопасности с учетом их доступа к данным и функциям Системы;
- Контроль за работоспособностью сервисов Системы, их перезапуск в случае нештатных остановов, уведомление Разработчика Системы о нештатных ситуациях и ошибках, возникающих при работе сервисов Системы;

- Анализ журналов ошибок Системы, уведомление Разработчика Системы об ошибках и нештатных ситуациях, возникающих при работе Системы;
- Устранение неполадок в Системе собственными силами, а в случае невозможности – с помощью СТП Разработчика Системы;
- Документирование всех произведенных действий.

Помимо перечисленного, Администратор Системы отвечает за стабильность, производительность и целостность баз данных Системы. Таким образом, совместно с Администратором аппаратного обеспечения, он осуществляет:

- Настройку СУБД и баз данных Системы;
- Контроль целостности БД Системы;
- Контроль резервного копирования БД Системы;
- Восстановление БД Системы из резервных копий.

6.4 Обязанности офицера безопасности

Офицер информационной безопасности отвечает за обеспечение информационной безопасности компании.

Обязанностями офицера безопасности являются:

- Ответственность за информационную безопасность в организации;
- Защита ПО встроенными средствами и контроль доступа;
- Создание политик безопасности и политик карантина;
- Аудит и анализ событий информационной безопасности в Системе (журналы аудита), выявление и обработка инцидентов информационной безопасности.
- Оперативное реагирование в случае нарушений заданных политик;
- Документирование всех произведенных действий.
- Контроль соблюдения требований информационной безопасности, предъявляемых к Системе.

В организациях с большим штатом сотрудников, вышеупомянутые обязанности могут делиться между несколькими офицерами безопасности, например, сотрудниками, закрепленными за разными отделами организации.