методические материалы ProLAN

Должностные обязанности администратора сети

Оглавление

В данном документе вы найдете должностную инструкцию и развернутое описание должностных обязанностей системного администратора (администратора сети) в части оперативного управления IT-инфраструктурой. Документ может использоваться в качестве «рыбы» при разработке должностной инструкции администратора сети в компаниях среднего бизнеса (50-500 компьютеров).

Наряду с оперативным управлением IT-инфраструктурой, в обязанности администратора сети, как правило, входит стратегическое управление IT-инфраструктурой. Развернутое описание обязанностей по стратегическому управлению IT-инфраструктурой в данный документ не входит.

Компания ProLAN выполняет работы по адаптации данного документа к конкретному штатному расписанию и структуре IT-службы компании, а также осуществляет оценку профессиональной компетентности IT-персонала.

Компания ProLAN оказывает услуги по стратегическому управлению IT-инфраструктурой организации, а также техническому руководству, обучению и экспертной поддержке администратора сети компании. Кроме этого, ProLAN оказывает профессиональные услуги по подбору IT-персонала и IT-аутсорсингу. Подробнее – www.prolan.ru/hr

1. Должностная инструкция администратора сети как формальный документ (для HR-директора)

В соответствии с Трудовым Кодексом РФ должностная инструкция является локальным факультативным нормативным актом. Тем не менее, во многих компаниях должностная инструкция является обязательным документом, регламентирующим права и обязанности сотрудников компании. Обычно должностные инструкции разрабатываются HR-директором компании. Ниже приводится должностная инструкция администратора сети в том виде, в каком ее хотели бы видеть большинство HR-директоров.

1.1 Общие положения

1. Администратор сети (системный администратор) относится к категории специалистов.
2. Целью администратора сети является обеспечение требуемого качества работы пользовательских приложений, используемых для поддержки бизнес процессов компании (см. примечание 1).
3. Администратор сети должен знать:
   - Основные принципы функционирования IT-Инфраструктуры и составляющих ее компонент.
   - Общие положения промышленных стандартов, регламентирующих правила построения, тестирования и эксплуатации структурированных кабельных систем (EIA/TIA 568, 569, 606, TSB 67, TSB 72).
   - Общие принципы работы и параметры настройки сетевых протоколов, используемых в корпоративной сети (протоколы стека TCP/IP, CSMA/CD, ADSL, протоколы маршрутизации и т.п.).
   - Принципы настройки, оптимизации и устранения неполадок в работе базовых сетевых сервисов, используемых в корпоративной сети (файловый сервис, почтовый сервис, сервис БД, сервис доступа в Internet и т.п.).
   - Принципы администрирования баз данных, используемых в корпоративной сети.
   - Технико-эксплуатационные характеристики, принципы настройки и технической эксплуатации активного сетевого оборудования, используемого в корпоративной сети.
   - Принципы обеспечения информационной безопасности и антивирусной защиты корпоративной сети.
   - Языки программирования (Basic, VB Script, JScript и т.п.).
4. Администратор сети должен уметь:

- Работать с прикладным программным обеспечением, используемым в корпоративной сети (офисными приложениями, системами управления предприятием, справочными системами и т.п.).
- Работать с системным программным обеспечением, в том числе, предназначенным для управления IT-Инфраструктурой, обеспечения информационной безопасности, обеспечения антивирусной защиты и т.п.
- Выполнять мелкий ремонт активного и пассивного сетевого оборудования, модернизацию структурированной кабельной системы.
- Писать простые программы на языках программирования.

5. Администратор сети должен быть ознакомлен:
   - С правилами внутреннего трудового распорядка.
   - С правилами и нормами охраны труда, техники безопасности, производственной санитарии и противопожарной защиты.
   - С постановлениями, распоряжениями, приказами, и другими руководящими и нормативными документами, имеющими отношение к его должностным обязанностям.
   - С основными положениями корпоративной политики в области использования IT-инфраструктуры.

6. Назначение на должность администратора сети и освобождение от должности производится приказом директора компании.

7. Администратор сети подчиняется директору IT-службы (или руководителю компании).

8. На время отсутствия администратора сети (отпуск, болезнь, пр.) его обязанности выполняет лицо, назначенное в установленном порядке. Данное лицо приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.2 Ответственность администратора сети

1. Администратор сети несет ответственность за:
   - Обеспечение требуемого качества работы пользовательских приложений, используемых для поддержки бизнес процессов компании (см. примечание 1).
   - Обеспечение информационной безопасности и антивирусной защиты корпоративной сети.
   - Обеспечение защиты данных от разрушения в случаях сбоев в работе корпоративной IT-инфраструктуры и восстановление данных после сбоев.
   - Обеспечение конфиденциальности данных, хранящихся на корпоративных серверах сети.

Примечание 1. Качество работы пользовательских приложений определяется четырьмя основными характеристиками: производительность приложения, доступность приложения, время реакции приложения, время восстановления работы приложения после отказа IT-инфраструктуры. Обычно эти характеристики оговариваются в Соглашении об Уровне Обслуживания (SLA, Service Level Agreement). Подробнее об этих характеристиках можно прочесть в разделе «Технология SLa-ON» - www.prolan.ru/slaon .

2. Администратор сети привлекается к ответственности:
   - За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, - в пределах, установленных действующим трудовым законодательством Российской Федерации.
   - За правонарушения, совершенные в процессе своей деятельности, - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

- За причинение материального ущерба организации - в пределах, установленных действующим трудовым и гражданским законодательством Российской Федерации.

1.3 Должностные обязанности администратора сети

В обязанности администратора сети входит выполнение следующих работ:

1. Мониторинг основных показателей «здоровья» IT-инфраструктуры (см. примечание 2).
2. Оказание технической поддержки пользователям сети, в том числе, устранение дефектов IT-инфраструктуры (см. примечание2);
3. Подключение и отключение пользователей сети.
4. Установка, подключение и отключение аппаратных средств.
5. Инсталляция и контроль над используемыми программными средствами.
6. Контроль над выполнением (выполнение) резервного копирования данных.
7. Контроль защиты, обеспечивающей информационную безопасность компании.
8. Курирование и приемка работ, выполняемых сторонними организациями.
9. (**Опционально**) Стратегическое управление «здоровьем» IT-инфраструктуры (определение «узких мест», прогнозирование нагрузки и планирование производительности, разработка стратегии и внедрение системы управления IT-инфраструктурой, системы обеспечения информационной безопасности, системы архивирования данных и т.п.)

Примечание 2. Под «здоровьем» IT-инфраструктуры будем понимать доступность оборудования и сервисов, производительность оборудования и IT-сервисов, качество получаемых IT-сервисов, непрерывность IT-сервисов. Под «дефектом» IT-инфраструктуры будем понимать неисправное активное и пассивное оборудование, неверные параметры настройки активного оборудования и программного обеспечения, устаревшую «прошивку» (firmware) активного оборудования, устаревшие версии системного программного обеспечения и т.п.

1.4 Права администратора сети

Администратор сети имеет право:

1. Требовать от руководства компании обеспечения организационно-технических условий, необходимых для исполнения своих должностных обязанностей том числе, приобретение требуемого инструментария, оплата обучения и т.п.
2. Информировать руководство компании о невозможности нести возложенную на него ответственность вследствие объективных (независящих от него) причин.
3. Отключать пользователей сети, действия которых противоречат корпоративной политики пользования IT-Инфраструктурой и/или могут негативно повлиять на информационную безопасность, антивирусную защиту, производительность или надежность работы корпоративной сети.
4. Вносить на рассмотрение руководства компании предложения по улучшению работы IT-инфраструктуры.
5. Устанавливать и изменять правила пользования IT-инфраструктурой, в частности, пароли доступа к различным ресурсам сети.

2. Оперативное и Стратегическое управление IT-инфраструктурой

Следует выделить два вида управления IT-инфраструктурой: оперативное управление и стратегическое управление. В рамках оперативного управления решаются задачи, требующие быстрой (оперативной) реакции IT-персонала. В рамках стратегического управления решаются задачи, требующие анализа данных о работе IT-инфраструктуры.

Если процесс управления IT-инфраструктурой организован правильно, оперативным и стратегическим управлением должны заниматься разные специалисты. По нашему мнению, администратор сети должен заниматься только вопросами оперативного управления и НЕ ДОЛЖЕН заниматься стратегическим управлением. Стратегическое управление должно быть в зоне ответственности руководителя IT-службы, или в штатном расписании должна быть предусмотрена соответствующая позиция.

Если компания небольшая и администратор сети является единственным IT-специалистом, вопросы стратегического управления целесообразно передать на аутсорсинг внешней компании (системному интегратору), имеющей опыт решения таких задач. Иначе велика вероятность того, что задачи стратегического управления не будут решаться должным образом, и IT-инфраструктура будет развиваться стихийно.

Оперативное управление IT-инфраструктурой включает в себя выполнение следующих работ:

- мониторинг основных показателей «здоровья» IT-инфраструктуры (см. примечание2);
- оказание технической поддержки пользователям сети, в том числе, устранение дефектов IT-инфраструктуры (см. примечание 2);
- подключение и отключение пользователей сети;
- установка, подключение и отключение аппаратных средств;
- инсталляция и контроль над используемыми программными средствами;
- контроль над выполнением (выполнение) резервного копирования данных;
- контроль защиты, обеспечивающей информационную безопасность компании;
- (опционально) курирование и приемка работ, выполняемых сторонними организациями.

Примечание 2. Под «здоровьем» IT-инфраструктуры будем понимать доступность оборудования и сервисов, производительность оборудования и IT-сервисов, качество получаемых IT-сервисов, непрерывность IT-сервисов. Под «дефектом» IT-инфраструктуры будем понимать неисправное активное и пассивное оборудование, неверные параметры настройки активного оборудования и программного обеспечения, устаревшую «прошивку» (firmware) активного оборудования, устаревшие версии системного программного обеспечения и т.п.

Стратегическое управление IT-инфраструктурой включают в себя выполнение следующих работ:

- разработка критериев «здоровья» IT-инфраструктуры;
- внедрение системы управления «здоровьем» IT-инфраструктуры;
- определение «узких мест» IT-инфраструктуры (см. примечание 3);
- разработка стратегии и внедрение системы архивирования данных;
- разработка стратегии и внедрение системы обеспечения информационной безопасности;
- планирование развития IT-инфраструктуры, в частности, планирование утилизации (процента использования) системных ресурсов (вычислительных ресурсов, пропускной способности каналов связи, объема дискового пространства и т.п.);
- планирование бюджета на развитие IT-инфраструктуры;
- документирование ключевых показателей «здоровья» IT-инфраструктуры.

Примечание 3. Под «узким местом» IT-инфраструктуры будем понимать любой системный ресурс, высокая утилизация которого оказывает негативное влияние на время реакции и производительность пользовательских приложений. Примерами «узких мест» является производительность сервера, пропускная способность канала связи и т.п.

3. Мониторинг основных показателей «здоровья» IT-инфраструктуры

Цель мониторинга

Целью мониторинга «здоровья» IT-Инфраструктуры является предотвращение сбоев в работе пользовательских приложений и минимизация времени простоя IT-инфраструктуры, являющегося

следствием сбоев в работе активного и пассивного оборудования. При правильной организации процесса мониторинга сети, администратор сети (АС) узнает о возникновении сбоев не от пользователей, а на основании сообщений системы сетевого управления.

Технология проведения мониторинга

Для осуществления постоянного мониторинга «здоровья» IT-инфраструктуры АС должен иметь в своем распоряжении систему сетевого управления. Примером такой системы является пакет ProLAN NPM Analyst. Подробнее об этом пакете можно прочесть в [1].

Основные критерии «здоровья» IT-инфраструктуры, определенные в рамках стратегического управления IT-инфраструктурой, в качестве пороговых значений (thresholds) или значений базовой линии (base line) вводятся в систему сетевого управления. Описание и пороговые значения основных характеристик «здоровья» IT-инфраструктуры можно найти на web-сайте компании ProLAN в разделе «оценочные тесты», см. [2].

Систематическое и/или длительное превышение характеристиками «здоровья» IT-инфраструктуры пороговых значений или резкое отклонение от базовой линии свидетельствует об инциденте, причина которого должна быть установлена АС и, по возможности, устранена. Однократные (единовременные) превышения пороговых значений, как правило, инцидентами не считаются.

Возникновение инцидента документируется системой управления, и АС получает соответствующее уведомление (по электронной почте, пейджеру, и т.п.) Получив уведомление, АС должен оценить уровень важности произошедшего инцидента и сделать соответствующую запись в **Журнале Инцидентов и Работ** (далее **ЖИР**). Запись в ЖИР может делаться вручную или автоматически (средствами системы сетевого управления). Если важность инцидента высокая, АС должен незамедлительно приступить к его устранению.

Если для устранения инцидента требуется приобретение (получение со склада) оборудования или материалов, АС составляет Требование (документ установленной формы), которое подписывается непосредственным начальником АС, например, директором информационной службы (CIO).

Отчетность

Все работы по устранению инцидентов, выполняемые АС, должны фиксироваться в ЖИР. Для каждого инцидента в ЖИР должна заноситься следующая информация:

- Порядковый номер инцидента.
- Дата и время возникновения инцидента.
- Название инцидента (как проявляется), например, «недоступность сервера FS»
- Дата и время устранения инцидента.
- Что сделано для устранения инцидента.
- (Опционально.) Причина инцидента или комментарий.

ЖИР регулярно просматривается руководителем АС.

ПРИМЕЧАНИЕ. ЖИР является объективным показателем не только «здоровья» IT-инфраструктуры, но и качества выполняемых АС работ. Информация, содержащаяся в ЖИР, может являться основанием для премирования или «наказания» АС.

4. Оказание технической поддержки пользователям сети

Цель технической поддержки

Техническая поддержка пользователей осуществляется с целью минимизации времени простоя пользователей, вызванного невозможностью выполнения ими своих должностных обязанностей. Обучение пользователей работе с приложениями, как правило, выходит за рамки технической поддержки и должно оговариваться особо.

Технология осуществления технической поддержки

Для осуществления технической поддержки пользователей, АС должен иметь в своем распоряжении эффективный диагностический инструментарий (кабельный тестер/сканер, анализатор протоколов/трафика и т.п.) Информацию о кабельных тестерах кампании Fluke можно найти в [3]. Информацию о кабельных тестерах кампании Agilent можно найти в [4]. Описание анализатора протоколов Observer компании Network Instruments можно найти в [5]. Для технической поддержки пользователей в крупных IT-инфраструктурах желательно наличие в компании приложения типа Help Desk.

Невозможность пользователя выполнить сетевую операцию считается инцидентом, причина которого должна быть установлена и устранена АС. Пользователь, нуждающейся в технической поддержке, обращается к АС и сообщает ему о возникшей проблеме. В простейших случаях обращение производится в устной форме (по телефону) или в письменной форме (по электронной почте). Если в компании используется приложение типа Help Desk, пользователь заполняет экранную форму этого приложения.

Получив обращение пользователя, АС должен сделать соответствующую запись в ЖИР. Если в компании используется приложение типа Help Desk, запись делается пользователем самостоятельно. Как правило, все инциденты, вызванные обращениями пользователей, имеют высокий приоритет, и АС должен незамедлительно приступить к выяснению их причины. (Если в компании используется приложение типа Help Desk, пользователь может самостоятельно установить важность инцидента). Выяснения причин инцидентов осуществляется АС с использованием диагностического инструментария.

В рамках выполнения работ по поддержке пользователей, АС должен выполнять работы по устранению дефектов IT-инфраструктуры, не требующие ремонта её компонент или узлов. Устранение дефектов, как правило, выполняется методом замены неисправных компонент и/или узлов IT-инфраструктуры. Например, АС должен выполнять замену вышедших из строя фрагментов кабельной системы сети, замену неисправных сетевых плат, мониторов, принтеров и т.п., и организовать их ремонт. Проведение их ремонта собственными силами, как правило, выходит за рамки должностных обязанностей АС.

Если для устранения инцидента требуется приобретение или получение со склада оборудования, материалов, или оплата услуг сторонней организации (например, ремонтной мастерской), АС составляет **Требование** (документ установленной формы), которое подписывается непосредственным начальником АС.

Отчетность

Все работы по оказанию поддержки пользователям, выполняемые АС, должны фиксироваться в ЖИР. Для каждого инцидента в ЖИР должна быть занесена следующая информация:

- Порядковый номер инцидента.
- Дата и время возникновения инцидента.
- Название инцидента (как проявляется), например, невозможность распечатать документ.
- Дата и время устранения инцидента.
- Что сделано для устранения инцидента.
- (Опционально.) Причина инцидента или комментарий.

ЖИР регулярно просматривается непосредственным начальником администратора сети.

При правильной организации процесса администрирования сети число обращений пользователей для оказания технической поддержки минимально, т.к. АС узнает о возникновении инцидентов не от пользователей, а на основании показаний системы сетевого управления. Это позволяет ему, во-первых, узнавать об инцидентах раньше, чем они скажутся на работе пользователей, во-вторых, предотвращать возникновение инцидентов.

5. Подключение и отключение пользователей сети

Цель подключения и отключения пользователей

Пользователи подключаются к сети с целью обеспечения возможности доступа к разделяемым ресурсам сети (базам данным, серверам, принтерам, Internet-каналам и т.п.). Пользователи отключаются от сети с целью прекращения возможности доступа к ресурсам сети. При правильной организации процесса администрирования сети пользователи имеют доступ только к тем ресурсам, которые им необходимы для выполнения своих должностных обязанностей.

Технология подключения и отключения пользователей

Для подключения и отключения пользователей, как правило, достаточно возможностей штатных программных средств, входящих в состав системного программного обеспечения.

Для подключения (отключения) пользователей к серверам, как правило, используются программы, входящее в состав операционных систем. Например, для MS Windows 2000 - это MMC консоль с оснасткой - Active Directory Users and Computers. Для Novell NetWare – программа ConsoleOne. Для подключения пользователя к конкретному серверу, АС, как правило, должен установить следующие параметры:

- имя пользователя;
- пароль доступа;
- время до следующего изменения пароля;
- права для доступа к ресурсам сети.

В ряде случаев для обеспечения доступа к Internet, почтовым системам, базам данных и т.п., АС должен использовать специальные программы, поставляемые совместно с соответствующим оборудованием или программным обеспечением. Например, для обеспечения доступа к Internet может потребоваться настройка маршрутизаторов сети, для заведения почтового ящика – настройка почтовой системы и т.д.

Отчетность

Все работы по подключению и отключению новых пользователей должны фиксироваться в ЖИР. Кроме этого, АС должен поддерживать в актуальном состоянии **Паспорт Сети**, включающий в себя, в том числе, следующую информацию:

- список существующих групп с правами доступа к ресурсам сети;
- список пользовательских аккаунтов и их членство в группах.

Пример Паспорта Сети можно найти в [6].

6. Установка, подключение и отключение аппаратных средств

Цель подключения аппаратных средств

При правильной организации процесса администрирования сети только АС (или другое уполномоченное лицо) имеет право подключать, отключать или изменять параметры настройки аппаратных средств. Необходимость подключения и отключения аппаратных средств определяется руководителем АС.

Технология подключения и отключения аппаратных средств

Для проверки правильности работы аппаратных средств, подключаемых к сети, АС желательно иметь генератор сетевого трафика, который может быть программным или аппаратным. Примерами программных генераторов трафика являются программы ProLAN FTest, ProLAN NPM Probe+, NetIQ Chariot. Описание программы ProLAN FTest можно найти в [7]. Описание программы ProLAN NPM Probe+ можно найти в [8].

При правильной организации процесса администрирования сети процедура подключения аппаратных средств определяется для каждого типа устройства и утверждается директором информационной службы. Обычно такая процедура включает в себя пять основных этапов.

- Проверка установленной версии внутренней «прошивки» (firmware) и при необходимости ее модернизация (upgrade).
- Установка идентификатора устройства (IP-адреса, имени) в соответствии с утвержденным планом идентификации устройств данного типа.
- Проверка параметров настройки устройства, установленных по умолчанию, и при необходимости, их изменение.
- Внесение информации о подключаемом устройстве в Паспорт Сети [6].
- Тестирование подключенного устройства; обычно тестирование заключается в создании генератором трафика высокой нагрузки на подключаемое устройство и измерении характеристик «здоровья» устройства и/или сети (числа ошибок передачи данных, скорости передачи данных, времени реакции сети и т.п.)

При отключении устройства от сети АС должен внести соответствующую информацию в Паспорт Сети.

Документирование и отчетность

Все работы по подключению и отключению аппаратных средств должны фиксироваться в ЖИР. Кроме этого, АС должен поддерживать в актуальном состоянии Паспорт Сети, включающий в себя, в том числе, следующую информацию:

- карту топологии сети;
- идентификаторы устройств сети;
- версии firmware и прошивок, используемых в оборудовании;
- отчеты о «здоровье» активного сетевого оборудования;
- конфигурацию серверов и рабочих станций, подключенных к сети

Пример Паспорта Сети можно найти в [6].

7. Инсталляция и контроль над используемыми программными средствами

Цели инсталляции и контроля над программными средствами

При правильной организации процесса администрирования сети только АС (или другое уполномоченное лицо) имеет право устанавливать программные средства, в том числе, на компьютеры пользователей сети. Необходимость инсталляции программных средств определяется руководителем АС. Политика информационной безопасности, как правило, запрещает пользователям сети самостоятельно устанавливать и/или использовать какие-либо приложения, кроме

санкционированных, т.е. тех, которые необходимы им для выполнения своих должностных обязанностей.

Контроль над программными средствами, запущенными (и/или установленными) на рабочих станциях пользователей сети, позволяет выявить следующие факты:

- факты несанкционированной инсталляции приложений;
- факты использования нелицензионных программ;
- факты использования приложений, которые могут нанести вред IT-инфраструктуре;
- факты не целевого использования рабочего времени (компьютерные игры в рабочее время и т.п.).

Инсталляция программных средств

Современные операционные системы имеют все необходимые средства для автоматического, централизованного распространения (инсталляции) программных средств на рабочие станции сети. Например, в операционной системе MS Windows 2000 для этих целей можно использовать расширение Software Installation, с помощью которого АС может автоматически устанавливать все необходимые приложения.

Контроль над используемыми программными средствами

Для осуществления контроля над используемыми программными средствами АС должен иметь в своем распоряжении специальные программы управления приложениями. Примерами программ управления приложениями являются пакеты ProLAN NPM Analyst [1] и NetIQ Security Manager.

Запуск пользователем сети несанкционированного приложения считается инцидентом, о котором должен быть поставлен в известность АС. Перечень несанкционированных приложений утверждается директором информационной службы. АС вводит список несанкционированных приложений в программу управления приложениями. Программа управления приложениями автоматически контролирует все запущенные приложения и при обнаружении работающих несанкционированных приложений, автоматически информируют об этом АС. Некоторые программы управления приложениями (например, ProLAN NPM Analyst) могут автоматически терминировать несанкционированные приложения.

Документирование и отчетность

Все работы по установке и удалению программных средств должны фиксироваться в ЖИР. Кроме этого, АС должен регулярно, не реже одного раза в квартал, создавать отчеты по инцидентам, связанным с запуском пользователями сети несанкционированных приложений. По каждому инциденту, имевшему место за отчетный период, АС должен фиксировать следующую информацию:

- дата и время инцидента;
- имя компьютера (имя пользователя), на котором произошел инцидент;
- название несанкционированного приложения, например, «запуск ICQLite.exe (ICQ)».

8. Контроль над выполнением (выполнение) резервного копирования данных

Цель резервного копирования данных

Резервное копирование данных является частью стратегии архивирования данных, включающей в себя план восстановления данных после аварий (disaster recovery plan). Обычно такая стратегия разрабатывается в рамках стратегического управления IT-инфраструктурой и утверждается

директором информационной службы. Целью архивирования данных является обеспечение непрерывности бизнес процессов компании. Резервное копирование позволяет обеспечить защиту данных от разрушения в случае сбоев аппаратных или программных средств, и/или в случае ошибок, допущенных пользователями сети.

Технология резервного копирования данных

Для организации резервного копирования данных в распоряжении АС должны быть специализированные аппаратно-программные средства, определенные в рамках стратегического управления IT-инфраструктурой.

Обычно процедура резервного копирования данных включает в себя следующие действия:

- определение и конфигурирование источников данных для резервного копирования (рабочие станции пользователей, сервера и т.д.);
- определение и конфигурирование устройств и носителей для сохранения резервируемых данных;
- настройка расписания для системы резервного копирования (что, куда и когда);
- контроль над выполнением резервного копирования.

Обычно план восстановления данных после аварий включает в себя следующие действия:

- оценка масштаба аварии для определения потерянных данных;
- нахождения наиболее актуальных резервных копий потерянных данных;
- физическое восстановление потерянных данных из копий;
- проверка восстановленных данных.

Документирование и отчетность

Все работы по организации резервного копирования данных должны фиксироваться в ЖИР. Обычно АС достаточно проверить, что резервное копирование данных произошло успешно и зафиксировать этот факт в ЖИР.

9. Контроль защиты, обеспечивающей информационную безопасность компании

Цель контроля

Контроль защиты является частью стратегии обеспечения информационной безопасности, разрабатываемой в рамках стратегического управления IT-инфраструктурой и утверждаемой директором информационной службы. Контроль выполняется с целью обеспечения непрерывной работы аппаратных и/или программных средств, выполняющих защитные функции.

Осуществление контроля

В рамках оперативного управления IT-инфраструктурой АС должен контролировать функционирование средств защиты. Обычно такой контроль включает в себя три составляющие:

- контроль защиты внешнего периметра сети;
- контроль антивирусной защиты серверов и рабочих станций;
- обеспечение своевременной установки исправлений (патчей) используемых в компании приложений и операционных систем.

В рамках контроля защиты внешнего периметра сети (маршрутизаторы, файрволы и т.п.) АС должен постоянно проводить мониторинг работоспособности (доступности) средств защиты,

своевременно обновлять их прошивку (firmware), а также производить их перенастройку согласно рекомендациям, получаемым от производителя средств защиты или компании, осуществляющей их поддержку.

В рамках контроля антивирусной защиты серверов и рабочих станций АС должен выполнять следующие действия:

- Своевременно обновлять сигнатуры вирусов, загружая их с web-сайта производителя средств антивирусной защиты.
- Своевременно устанавливать обновленные сигнатуры на рабочие станции пользователей сети.

В обязанности АС входит своевременная установка на все компьютеры сети обновлений (патчей) операционных систем и офисных приложений. При использовании ПО компании Microsoft для этих целей удобно использовать свободную программу MS Software Update Services (SUS).

Документирование и отчетность

Все работы по обеспечению информационной безопасности должны фиксироваться в ЖИР. Кроме этого, АС должен фиксировать в Паспорте Сети все изменения топологии, конфигурации и настройки аппаратных средств защиты (маршрутизаторов, файрволов и пр.), в том числе, изменение версий прошивки (firmware) оборудования, изменение файлов конфигурации и т. п.

10. Ссылки по теме

1. Описание пакета ProLAN NPM Analyst: www.prolan.ru/npmanalyst.
2. «Показатели здоровья IT-инфраструктуры» - описание оценочных тестов, поддерживаемых продуктами компании ProLAN: http://www.prolan.ru/solutions/technology/tests/index.html
3. Описание кабельных тестеров компании Fluke: http://www.prolan.ru/solutions/testing/fluke/index.html .
4. Описание кабельных тестеров компании Agilent: http://www.prolan.ru/solutions/testing/agilent/index.html
5. Описание анализатора протоколов Observer компании Network Instruments: http://www.prolan.ru/solutions/management/observer/index.html .
6. Пример Паспорта Сети – http://www.prolan.ru/netconsulting/description/netaudit/certificate.html
7. Описание программы ProLAN FTest: http://www.prolan.ru/ftest .
8. Описание программы ProLAN NPM Probe+: www.prolan.ru/npmprobe .
9. Описание технологии ProLAN SLa-ON: www.prolan.ru/slaon

Свои замечания, комментарии и предложения по данному документу Вы можете направлять по адресу hr@prolan.ru .