Государственное бюджетное дошкольное образовательное учреждение
детский сад № 27 комбинированного вида
Красногвардейского района Санкт-Петербурга

Принято
Общим собранием трудового
коллектива ГБДОУ детский сад
№ 27
Красногвардейского района СПб
Протокол № 1 от 07.02. 2019

Утверждаю :
Заведующий ГБДОУ
детский сад № 27
_____Е.Е.Мелешкина
« 07 » 02.2019г.
Приказ № 10/1-о
От 07.02.2019г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6635680065ADB8A64357E0855B692FE1
Владелец: Мелешкина Елена Евгеньевна
Действителен: с 14.07.2021 до 14.10.2022

ПОЛОЖЕНИЕ

о корпоративной компьютерной сети в

Государственном бюджетном дошкольном образовательном учреждении детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга

Санкт-Петербург

2019г.

Оглавление

Цель положения: *Определить основные функциональные аспекты сети, такие как: состав, структура, принцип действия, категории ресурсов; регламентировать организацию работ по сопровождению и развитию корпоративной сети; определить организационно-технические мероприятия, направленные на регламентацию работы пользователей и обслуживающего персонала, для обеспечения бесперебойной работы корпоративной компьютерной сети.*

Технические средства могут предоставлять различный уровень защиты от несанкционированного доступа и случайных сбоев, а так же обладать различными возможностями. Задача регламентирования работы с техническими средствами - это установление правил, обеспечивающих эффективность работы, необходимую безопасность и защиту информации.

1. Термины, определения и сокращения

- *Аппаратные средства* - это материальные объекты, используемые в технике.

- *Программные средства* - это программы, а также средства экранного и печатного представления - пользовательский интерфейс. Это нематериальные объекты.

- *Технические средства* включают аппаратные и программные средства. В данном документе рассматриваются только средства, относящиеся к компьютерам и сети.

- *Физическими устройствами* могут являться только аппаратные средства.

- *Логическими устройствами* являются программные средства, отождествляемые с соответствующими физическими устройствами.

- *Ресурсами* являются логические устройства и другие структуры представления данных для пользователя.

- *Сетевыми ресурсами* являются ресурсы, доступные через сеть.

- *Локальными ресурсами* являются ресурсы, доступные непосредственно на данном компьютере.

- *Защищаемая информация* - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями законодательных и иных нормативных документов или в соответствии с требованиями, устанавливаемыми собственником информации.

- *Категорирование защищаемых информационных ресурсов* - установление градаций важности обеспечения защиты (категорий) информационных ресурсов и отнесение конкретных информационных ресурсов к соответствующим категориям.

2. Назначение компьютерной сети

Корпоративная компьютерная сеть - это целостная структура вычислительных систем, состоящая из взаимодействующих сетей структурных подразделений. Нормальное функционирование корпоративной компьютерной сети требует реализации организационно-технических мероприятий, жесткой дисциплины пользователей и служб сопровождения.

Корпоративная компьютерная сеть является неотъемлемой частью системы управления и предназначена для решения научно-образовательных задач и задач управления на базе современных информационных технологий, обеспечивающих, в частности, ускорение принятия решений на основе:

- оперативного обмена данными между подразделениями ;
- использование общих информационных ресурсов размещенных в сети;
- доступа через единую компьютерную сеть к данным других интрасетей и глобальных сетей;
- использования электронной почты;
- организации централизованного хранилища данных с различным уровнем доступа к информации;
- отслеживание изменений данных в реальном масштабе данных.

Состав

Компьютерную сеть образуют базовые компоненты оборудования, программного обеспечения и параметров сетевого и межсетевого взаимодействия:

Сервер :

- файловые;
- баз данных;
- приложений;
- почтовые;
- архивные;
- удаленного доступа;
- печати.

Телекоммуникационная инфраструктура:

- кабели;
- соединительные устройства;
- устройства расширения (и ограничения) доступа;
- рабочие станции с необходимыми сетевыми адаптерами;
- системы дублирования и хранения информации;
- системы бесперебойного питания серверов и рабочих станций.

Информационная инфраструктура:

- операционные системы;
- протоколы сетевого и межсетевого взаимодействия;
- прикладное программное обеспечение коллективного доступа;
- прикладное программное обеспечение рабочих станций.

1 - Допускается использование одного сервера в качестве нескольких серверов различного назначения.

3. Структура названий средств вычислительной техники в сети

Структура названий средств персональной вычислительной техники в сети проистекает из необходимости уникального названия каждого персонального или мобильного устройства в сети, доступности восприятия обслуживающим персоналом, возможностью быстрого переименования и переподключения, а также учета средств вычислительной техники. Все настройки по именованию вычислительной техники в сети производятся сотрудниками по обслуживанию и ремонту средств ВТ.

Каждая рабочая станция имеет название вида Xxxxxxxxxx-AA-, где:

Xxxxxxxxxxx - название отдела, в котором установлено рабочее место;

AA - порядковый номер установленной рабочей станции. Рабочая станция руководителя отдела всегда имеет номер "01";

B - дополнительная маркировка в случае, когда рабочая станция является мобильной. В иных случаях не указывается.

В поле "Комментарии" обязательно должна быть указано название подразделения, за которым закреплена данная рабочая станция, и номер аудитории, где находится рабочая станция в данный момент. В случае движения техники, изменение комментария входит в обязанности сотрудника по обслуживанию и ремонту ВТ, устанавливавшего технику.

Структура названий сетевых принтеров - проистекает из необходимости уникального названия каждого принтера в сети, доступности восприятия обслуживающим персоналом, возможности быстрого переименования и пере- подключения в случае необходимости.

Каждый сетевой принтер имеет название вида A-BBB-CCCC-<DD>, где:

A - название корпуса

BBB - трехзначный номер комнаты, в которой установлен данный принтер. Если принтер установлен в коридоре, указывается ближайшая к нему комната;

CCCC - производитель принтера:

<DD> - дополнительная маркировка, указывающая на то, какой версией PCL пользуется принтер. По умолчанию драйвер принтера использует новейшую из возможных версий PCL. Если же по каким-либо причинам программное обеспечение требует более старой версии PCL, это необходимо указать в данном поле. Драйверы для принтеров, поддерживающих различные версии PCL, должны храниться в доступном месте на сервере.

Структура названия серверов в сети устанавливается непосредственно с согласием начальника отдела компьютерных коммуникаций по согласованию

с главным инженером. Все дополнительные сведения находятся в паспорте сервера и Active Directories.

Паспорт сервера представляет собой файл с аппаратными и программными характеристиками сервера, а также кратким описанием его назначения. Доступ к паспорту сервера в режиме чтения имеют сотрудники отдела, в режиме записи - администраторы сети. По письменному указанию главного инженера доступ к паспорту может быть предоставлен другим сотрудникам.

4.Принцип действия корпоративной сети

Функционирование сети обеспечивается подключением рабочих станций к серверам и объединением серверов посредством соединительной аппаратуры Расширение сети производится путем подключения дополнительных сегментов через маршрутизаторы, репитеры и каналы связи различного типа.

Подключение к всемирной сети Интернет производится через специализированные устройства и специализированное программное обеспечение для защиты внутренней сети от несанкционированного доступа ("взлома") извне.

Защита информации по уровням доступа производится путем администрирования файл-серверов и серверов БД и проведением специализированных организационно-технических мероприятий на основании категорирования ресурсов, описанных ниже.

Разделение единой сети на виртуальные зоны для обеспечения необходимого уровня безопасности осуществляется на основе стандарта IEEE 802.1Q (технология виртуальных сетей).

5.Категории защищаемых ресурсов

Категорирование информационных ресурсов (определение требований к защите ресурсов) является необходимым элементом работ по обеспечению информационной безопасности Государственного бюджетного дошкольного образовательного учреждения детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга и имеет своими целями:

- создание нормативно-методической основы для дифференцированного подхода к защите информационных ресурсов на основе их классификации по степени риска в случае нарушения их доступности, целостности или конфиденциальности;
- типизацию принимаемых организационных мер и распределения аппаратно-программных средств защиты информационных ресурсов по рабочим станциям и серверам Государственного бюджетного дошкольного образовательного учреждения детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга, а также унификацию вариантов настроек средств защиты.

Конфиденциальность информации - субъективно определяемое свойство информации, указывающее на необходимость введения ограничений на круг лиц, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней.

Категории конфиденциальности защищаемой информации:

- "СТРОГО КОНФИДЕНЦИАЛЬНАЯ" - к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства, а также информация, ограничения на распространение которой введены решениями руководства Государственного бюджетного дошкольного образовательного учреждения детский сад № 27 комбинированного вида Красногвардейского района Санкт-Петербурга (далее Организация), разглашение которой может привести к тяжким финансово-экономическим последствиям для Организации (нанесению тяжкого ущерба жизненно важным интересам её сотрудников, преподавателей, слушателей, партнеров);

- "КОНФИДЕНЦИАЛЬНАЯ" - к данной категории относится информация, не отнесенная к категории "СТРОГО КОНФИДЕНЦИАЛЬНАЯ", ограничения на распространение которой вводятся решением руководства Организации, разглашение которой может привести к значительным убыткам и потере конкурентоспособности Организации (нанесению ощутимого ущерба интересам её сотрудников, преподавателей, слушателей, партнеров);
- "ОТКРЫТАЯ" - к данной категории относится информация, обеспечения конфиденциальности которой не требуется.

Целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Категории целостности защищаемой информации:

- "ВЫСОКАЯ" - к данной категории относится несанкционированная модификация информации (искажение, подмена, уничтожение) или фальсификация (подделка), которая может привести к нанесению значительного прямого ущерба Организации, её сотрудникам, преподавателям, слушателей, партнерам. Целостность и аутентичность (подтверждение подлинности источника) которой должна обеспечиваться гарантированными методами;
- "НИЗКАЯ" - к данной категории относится несанкционированная модификация информации, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба Организации, её сотрудникам, преподавателям, слушателям, партнерам;
- "НЕТ ТРЕБОВАНИЙ" - к данной категории относится информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется.

Доступность информации - свойство системы обработки, информации в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов (пользователей) к интересующей их информации (при наличии у субъектов соответствующих полномочий на доступ) и готовность соответствующих автоматизированных служб (функциональных задач) к обслуживанию поступающих от субъектов запросов.

В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов их решения вводится четыре требуемых степени (категории) доступности функциональных задач. Задержки получения результатов могут быть связаны с аварийными ситуациями аппаратно-программного обеспечения, а

также как результат внешнего воздействия. К данным ситуациям не относятся форс-мажорные обстоятельства.

Требуемые степени доступности функциональных задач:

- "БЕСПРЕПЯТСТВЕННАЯ ДОСТУПНОСТЬ" - доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не должна превышать нескольких десятков минут);
- "ВЫСОКАЯ ДОСТУПНОСТЬ" - доступ к задаче должен осуществляться без существенных временных задержек (задача решается ежедневно, задержка получения результата не должна превышать нескольких часов);
- "СРЕДНЯЯ ДОСТУПНОСТЬ" - доступ к задаче может обеспечиваться с существенными временными задержками (задача решается раз в несколько дней, задержка получения результата не должна превышать нескольких дней);
- "НИЗКАЯ ДОСТУПНОСТЬ" - временные задержки при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата - несколько недель).

Информационное пространство разделено на 4 зоны по степени важности информации, и соответственно уровню их защиты с соответствующими критериями:

- *финансово-экономическая зона* содержит конфиденциальную информацию коммерческого характера, что делает её особо привлекательной для взлома. Вследствие этого к защите данной зоны должны быть предъявлены максимально возможные требования безопасности. Соответственно категории по конфиденциальности, целостности и доступности для этой зоны следующие: Строго конфиденциальная, высокая, высокая доступность.
- *административная зона* содержит информацию о внутреннем документообороте Организации в управленческих целях. Так как информация в этой зоне носит служебный характер и, предназначена

для определённых лиц, необходимо предусмотреть повышенные требования безопасности. Соответственно категории по конфиденциальности, целостности и доступности для этой зоны следующие: Строго конфиденциальная, высокая, средняя доступность.

- *образовательная зона* содержит ресурсы, предназначенные для учебного процесса. В данной зоне не содержится секретной информации, и требования к безопасности могут быть сведены к минимуму. Соответственно категории по конфиденциальности, целостности и доступности для этой зоны следующие: Открытая, нет требований, низкая доступность.
- *служебная зона* включает все серверы Организации и административные станции обслуживающего персонала корпоративной сети. Требования безопасности к этой зоне должны быть максимальными, но с учётом того, что эта зона должна предоставлять ресурсы конечным пользователям. Соответственно категории по конфиденциальности, целостности и доступности для этой зоны следующие: Строго конфиденциальная, высокая, беспрепятственная доступность.

Ответственность за присвоение категорий защищаемым информационным ресурсам конкретных рабочих станций (PC) возлагается на руководителей соответствующих подразделений Организации, которые непосредственно решают задачи на данных рабочих станциях и серверах.

Контроль за правильностью категорирования информационных ресурсов, располагаемых на защищенных серверах и рабочих станциях в подразделениях Организации осуществляется главным инженером.

Форма запроса размещения информационного ресурса группового пользования в корпоративной компьютерной сети, а также соотнесение данного ресурса к защищаемой категории представлена в Приложении 1.

6. Порядок работы с ресурсами корпоративной компьютерной сети

Общий порядок работы сети

Системные администраторы устанавливают правила работы с техническими средствами и правила использования общих ресурсов согласно возможностям, функциям, предназначению и степени защищенности этих средств, ресурсов и требованиям к защите и доступности информации, с которой производятся работы.

Системные администраторы определяют и вводят технические средства и ресурсы, предназначенные для работы с информацией, в соответствии с требованиями к защите и доступности этой информации согласно решению руководства.

Пользователи подчиняются правилам, устанавливаемым данным положением. Пользователи ответственны за несоблюдение правил и, как следствие, утрату и порчу информации, а также распространение ее за пределы, устанавливаемые требованиями к защите.

Требование по работе с техническими средствами:

Пользователям запрещается:

- самовольно производить сборку, разборку, установку и техническое обслуживание аппаратных средств, равно как установку, удаление, настройку и декомпиляцию программных средств;
- запускать и использовать программные средства помимо средств описанных в "Положении по стандартизации программного обеспечения";
- защищать данных, способами не согласованными с администраторами, равно как уничтожение ценных данных;
- хранение данных на серверах, в местах не согласованных с администраторами;
- разглашение информации открывающей доступ других лиц к техническим средствам и данным или передача средств доступа к ним;

- поиск средств и путей повреждения, уничтожения технических средств или преодоления их защиты, равно как использование таких средств.

Пользователи обязаны:

- выполнять процедуры и предосторожности, предписанные администраторами;
- сообщать обо всех обнаруженных случаях повреждения или отказа технических средств и их защиты начальнику отдела или главному инженеру.

Администраторы обязаны:

- разграничивать права доступа в соответствии с требованиями к защите и категорирования ресурсов;
- своевременно реагировать на сообщения об отказах, повреждениях технических средств и их защиты;
- действовать в интересах безопасности прежде, чем в интересах удобства работы пользователей.
- выставлять ограничения в соответствии с их возможностями.

Администраторы и пользователи должны бережно относиться к техническим средствам.

Для оптимизации функционирования компьютерной сети системный администратор имеет право анализировать работу любого элемента входящего в состав сети.

Для устойчивой работы сети в целом, рекомендации системного администратора по реконфигурированию элементов, входящих в состав сети, обязательны для исполнения пользователем.

Все неисправности в обязательном порядке регистрируются системным администратором в "Журнале работы корпоративной компьютерной сети", находящемся в лаборатории компьютерных коммуникаций.

Администрирование серверов производится системным администратором, в соответствии с должностной инструкцией.

Создание учетной записи пользователя и уровень его доступа к информации определяется проректором по информатизации Организации на основании служебной записки, и реализуются только системным администратором.

Новый пользователь обязан обосновать необходимость внесения его учетной записи в домен. Ему необходимо согласовать с администратором домена уникальный идентификатор, с которым он будет идентифицироваться в домене. Администратор в свою очередь должен предоставить пользователю пароль, который тот сможет изменить при первом входе в домен. Администратор домена может ограничить по времени и правам уникальный идентификатор пользователя в зависимости от конкретной ситуации.

Отключение серверов или рабочих станций для технологических целей производится только системным администратором с обязательным предварительным уведомлением всех пользователей ресурсов данного сервера или рабочей станции или в не рабочее время.

При отключении серверов или устранении на них возникших неисправностей, системный администратор обязан, в первую очередь, осуществить организационно-технические мероприятия (установка обходного пути, реплицирование БД и т.д.) по обеспечению неразрывности рабочего процесса подразделений.

Создание и сопровождение телекоммуникационных каналов сети является исключительной компетенцией Организации. Топология компьютерной сети документируется.

Подключение персональных компьютеров к сети производится только работниками по обслуживанию и ремонту ВТ по заявкам соответствующих подразделений согласованных с начальниками подразделений и главным инженером. Решение о подключении в корпоративную компьютерную сеть Организации или её реорганизация выполняется системным администратором на основании заявки и в соответствии с имеющимися ресурсами и техническими возможностями. Изменение топологии сети

сторонними организациями или самостоятельно пользователем, подключение и реконфигурация любого элемента сети без согласования с начальником отдела или главным инженером запрещено.

Подключение модемов и иных устройств на рабочих станциях для доступа в сеть извне запрещено. В исключительных случаях такие подключения осуществляет системный администратор на основании служебной записки по разрешению проректора по информатизации с обязательным контролем сотрудников лаборатории компьютерных коммуникаций этих рабочих станций.

Настройка операционной системы рабочих станций пользователей для корректной работы сети производится только работниками по обслуживанию и ремонту ВТ. Изменение конфигурации системы рабочих станций, установка новых программных продуктов и аппаратных средств, изменяющих настройки системы самостоятельно или сторонними лицами без участия администратора сетей Организации категорически запрещено.

Права и обязанности пользователей компьютерной сети регламентируются настоящим Положением и должностными инструкциями.

Отключение пользователя нарушившего правила работы в сети от сетевых ресурсов производится с обязательным уведомлением данного пользователя.

При любых изменениях конфигурации подключения пользователя системным администратором производится обязательная проверка функционирования канала и доступа к ресурсам сети.

Пользователям сети категорически запрещено передавать сторонним лицам какие-либо сведения о настройке элементов сети (как-то: имена пользователей, пароли и т.д.). Несанкционированное расширение пользователями своих или чужих прав запрещено. Запрещено изменять месторасположение рабочих станций без согласования с администратором сетей Организации и главного инженера по обслуживанию и ремонту средств ВТ.

В случае нарушения установленного порядка функционирования компьютерной сети виновные сотрудники на основании докладной записки администраторов сетей и по обслуживанию и ремонту ВТ будут привлекаться к административной и материальной ответственности.

7.Порядок парольной защиты

Учетная запись пользователя - это его реквизиты в сети, основные параметры которой есть имя и пароль пользователя. Управление учетными записями всех пользователей обеспечивают администраторы сети.

Учётная запись пользователя заводится администратором сетей с требованием изменения пароля учётной записи пользователем при следующем входе в систему.

Административными паролями обладают только системные администраторы соответствующих серверов и хранятся они в запечатанном конверте в сейфе начальника отдела и главного инженера Организации.

Права доступа в сети распределяются на основе учетных данных пользователей.

Пароль пользователя, в случае если он держится в секрете, гарантирует что:

- Никто другой не мог произвести действия, которые были зафиксированы системой как действия данного пользователя.
- Никто не мог получить доступ к защищаемой информации, воспользовавшись учетной записью пользователя;
- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.
- Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Если пользователю требуется доступ к данным другого пользователя, он может получить его с соответствующего разрешения, продолжая работать под своей учетной записью.

Если пользователю требуются возможности, которыми обладает компьютер другого пользователя, он может войти на нем под своей учетной записью.

Пользователь обязан сохранять свой пароль в тайне и вводить его самостоятельно.

Правила работы с учетными записями:

Пользователям заводятся, отключаются учетные записи и присваиваются соответствующие права по распоряжению проректора по информатизации.

Учетные записи подчиненных могут быть заблокированы на время отпуска по распоряжению непосредственного и любого вышестоящего руководителя, а так же отдела кадров.

Учетная запись подчиненного может быть временно заблокирована и разблокирована, либо изменено время доступа по ней через распоряжение начальника, если она не была заблокирована распоряжением вышестоящего начальника.

Администраторы обязаны записывать в журнал операции заведения, блокирования, удаления учетных записей пользователей и групп.

8.Порядок работы с документами

Руководитель подразделения (отдела) определяет, является ли документ необходимым только пользователю или другим сотрудникам и степень его конфиденциальности. Если документ впоследствии необходим другим пользователям, он может быть помещен в папку для групповой работы. Поместить документ в существующую папку пользователь может самостоятельно, а для создания новых групповых папок необходимо заполнить форму, описанную в приложении 1.

Изменение статуса пользователя или изменение использования им групповых ресурсов производится посредством оформления соответствующей формы (Приложение 2) руководителем подразделения, где работает сотрудник.

При начальной настройке рабочей станции сотрудниками по обслуживанию и ремонту ВТ создаётся папка "ОБЩИЕ" с доступом к ней для всех пользователей сети. Эта папка предназначена для размещения файлов для передачи другим лицам. Пользователь, помещающий файл в эту папку, несет ответственность за возможное нежелательное открытие информации, содержащейся в ней.

Для конфиденциальной передачи документов используется электронная почта. Отправляя документ по электронной почте, пользователь разрешает доступ к документу тому получателю, которому он его отправляет. Пользовательские почтовые ящики заводит администратор Интернет-серверов. Получить почтовый ящик Организации может любой сотрудник ГОУ ДПО ЦПКС СПб «РЦОКОиИТ» оформив соответствующую заявку (Приложение 3). Администратор Интернет-серверов обязан предоставить

пользователю все данные о почтовом ящике (имя, пароль, протоколы и порты доступа к почтовому ящику). Пользователь может через Web-интерфейс изменить пароль на доступ к почтовому ящику, в противном случае администратор Интернет- серверов не несет ответственности за сохранность и конфиденциальность информации. Администратор Интернет-серверов передает полные права на управление почтовым ящиком пользователю.

Правила работы с документами и папками для документов:

Все документы должны храниться в личных или общих папках (папках для групповой работы), определенных администраторами. Кроме этого документы для которых не действует регламентация по конфиденциальности, могут передаваться сотрудниками с помощью папки "ОБЩИЕ".

Доступ руководителя к документам подчиненного разрешается администраторами всегда.

Доступ пользователя или группы пользователей к каким-либо документам может быть разрешен только владельцем документов или руководителем группы (отдела, подразделения), которой принадлежат данные документы.

Документы, имеющие отношение только к группе и требующие доступа со стороны всех членов группы, должны храниться исключительно в папке группы.

Папки для публикаций предназначены для предоставления материалов группы (отдела, подразделения) для общего использования, они открыты на чтение для всех, но на запись только для группы, ведущей данную папку.

9.Порядок работы с базами данных

Права доступа к средствам и операциям работы с базами данных, так же как и сами средства, определяются разработчиками баз данных. Администраторы и пользователи действуют на основании инструкций и документации, составленных разработчиком.

Пользователи не имеют права осуществлять самовольное копирование и сохранение баз данных.

10.Порядок работы с электронной почтой

Все пользователи, для обеспечения рабочих потребностей имеют адрес и ящик электронной почты. Пользователи должны понимать, что при отправке и получении почты через Интернет, её конфиденциальность не обеспечивается. *При обмене по электронной почте действуют следующие правила:*

- Пользователи должны использовать электронную почту только для передачи сообщений и документов, но не программ.
- Администраторы могут выдвигать дополнительные требования по содержимому сообщений, обусловленные соображениями совместимости форматов сообщений и документов, пересылаемых по электронной почте, как для внутреннего, так и для внешнего обмена.

11.Порядок антивирусной защиты

Использованию в Организации допускаются только лицензионные антивирусные средства, централизованно закупленные главным инженером у разработчиков (поставщиков) указанных средств.

Установка средств антивирусного контроля на серверах корпоративной компьютерной сети Организации осуществляется системными администраторами соответствующих серверов. Установка средств антивирусного контроля на рабочих станциях пользователей осуществляется сотрудниками (системными администраторами) по обслуживанию и ремонту средств ВТ. Настройка параметров средств антивирусного контроля осуществляется системными администраторами в соответствии с руководствами по применению конкретных антивирусных средств.

Ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов PC.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере, или при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо

проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов);
- Ответственным за организацию и проведение антивирусного контроля на серверах Интернет и внешнем шлюзе назначается администратор серверов Интернет главным инженером Организации.

Ответственным за организацию и проведение антивирусного контроля на серверах корпоративной сети назначается администратор корпоративных серверов из состава Организации.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на всех пользователей корпоративной сети.

Приложение №1

Форма запроса размещение на сервере информационного ресурса группового использования в корпоративной компьютерной сети

Прошу создать групповую папку

_____

Параметры групповой папки

_____

Назначение групповой папки

_____

Имя групповой папки

_____

Ответственный за сопровождение групповой папки

_____

Для кого должна быть доступна:

_____
_____
_____
_____
_____

Пути доступа к групповой папке (заполняется сотрудником ЛКК) Имя

Имя

_____
_____

Путь

_____
_____

Путь доступа к групповой

_____

сервера _____

тома _____

к папке _____

папке в корпоративной сети

_____

_____

_____

_____

Значение атрибутов доступа к групповым папкам (заполняется ответственным за сопровождение групповой папки) Имя группы пользователей (или пользователя)

Имя групповой папки или файла _____

Права доступа _____

(чтение или запись)

/_____/ _____

подпись Ф.И.О.

"___"_____ 20__ г

Согласовано:

Приложение №2

Форма изменения доступа сотрудника к информационным ресурсам группового пользования

Прошу внести изменения для доступа к групповой папке Имя группы пользователей (или пользователя)

Имя групповой папки или файла

_____

Права доступа

_____

(чтение или запись)

/_____/ _____

подпись Ф.И.О.

"___"_____ 20__ г

Приложение №3

Форма заявки на создание почтового ящика на сервере mail.domen.ru

Прошу создать почтовый ящик на сервере организации.

Почтовый адрес _____@domen.ru

Настоятельно рекомендуем вам сменить пароль (пароль по умолчанию соответствует почтовому адресу до @).Это возможно сделать, запустив обозреватель Интернета, зайти по адресу mail.domen.ru, указать почтовый адрес и пароль. Адрес почтового сервера POP3 и SMTP - mail.domen.ru

Приложение №4.

Профилактические работы

Таблица №1

Категории профилактических работ

Ежедневные работы

_____

_____

_____

_____

_____

Еженедельные работы

_____

_____

_____

_____

_____

Декадные работы

_____

_____

_____

_____

_____

Ежемесячные работы

_____

_____

_____

_____

_____

Анализ Интернет-траффика

_____

_____

_____

Проверка сетевого взаимодействия

_____

Проверка целостности операционной системы

_____

Составление отчета доступа к Интернет-ресурсам_____

_____

_____

_____

_____

Анализ возможностей доступа пользователей к сетевым ресурсам

Профилактика баз данных

_____

Принудительная проверка отказоустойчивости системы

_____

_____

_____

Удаление временных и устаревших копий файлов_____

_____

_____

_____

Просмотр отчетов служебных программ

_____

_____

_____

_____

Проверка наличия обновлений операционной системы и серверных приложений_____

_____
_____
_____

Профилактика дисковой и файловой подсистем на сервере
_____

_____
_____
_____

Анализ журналов событий серверов
_____

Проверка работы сервисов и служб
_____

Выполнение прочих работ, непосредственно связанных с работоспособностью рабочих станций

_____
_

_____
_____
_____
_____

Анализ отчетов системы безопасности
_____

Антивирусная профилактика сервера
_____

Профилактический останов сервера
_____

_____
_____
_____
_____

Проверка работоспособности почтовых служб и служб Интернета

Проверка времени последнего обновления антивирусных баз на рабочих станциях

Выявление попыток несанкционированной установки приложений на рабочих станциях

Удаление временных и устаревших копий файлов

Таблица 2

.Перечень проведенных профилактических работ за _____ 20__г

Дата

_____

Идентификатор компьютера

_____

Планируемые профилактические работы

_____

_____

_____

_____

_____

Фактически выполненные работы

_____

_____

_____

_____

Ожидаемый результат

_____

_____

_____

Лицо, проводившее профилактику

_____