г.Москва
Распоряжение от 18 января 2008 года № 22-рп

О результатах работ по созданию системы защиты информации за 2006-2007 гг. и задачах на 2008 г.

Принято
Префектом Зеленоградского административного округа г. Москвы

Во исполнение распоряжений префекта от 04.02.2005 N 120-рп "Об итогах работы по обеспечению технической защиты информации в 2004 году и задачах на 2005 год", от 01.07.2005 N 651-рп "О ходе работ по созданию системы защиты информации", от 30.06.2006 N 686-рп "О результатах работ по созданию системы защиты информации за 2005 г. и I кв. 2006 г. и задачах на 2006-2007 гг." в 2006-2007 гг. в префектуре был проведен комплекс мероприятий по обеспечению безопасности при обработке информации в вычислительных сетях. Для повышения физической защищенности серверного оборудования введен в эксплуатацию центр обработки данных префектуры, проведены мероприятия по ограничению доступа в серверную префектуры с помощью электронных карт, утвержден список сотрудников и определены права доступа в серверное помещение префектуры. Закуплены, подключены и настроены ленточная библиотека и дисковая система хранения данных. В рамках соглашения N 506/2007 от 05.12.2007 между префектурой Зеленоградского АО и обществом с ограниченной ответственностью "Майкрософт Рус" о взаимном сотрудничестве в декабре 2007 года начаты работы по внедрению системы мониторинга программно-аппаратной инфраструктуры префектуры.

Ведется постоянный контроль над актуальным уровнем доступа пользователей к сетевым и информационным ресурсам префектуры. В октябре 2007 года проведены комплексные проверки префектуры и подведомственных организаций на следование правилам безопасности при обработке на компьютерах информации ДСП.

В целях выполнения поручений распоряжения Правительства от 05.12.2007 N 2676-РП "О вводе в промышленную эксплуатацию первой очереди системы мониторинга информационных систем города Москвы и определение порядка ее функционирования", дальнейшего повышения безопасности при передаче, обработке и хранении информации на средствах вычислительной информации:

1. Одобрить результаты работ по развитию системы защиты информации за 2006-2007 гг.
2. Отделу службы "одного окна" и информатизации (Коробова А.Н.) в срок до 01.03.2008 завершить установку и настройку системы мониторинга событий, состояния и производительности серверных и пользовательских программно-аппаратных ресурсов префектуры (далее - СМС). В срок до 01.04.2008 организовать настройку через СМС профиля автоматизированных рабочих мест префектуры в соответствии с приложением 1.
3. Главам управ районов Матушкино-Савелки, Панфиловского, Крюково (Ласточкин В.П., Чеботарев А.В., Бодаданов Д.А.) совместно с начальником службы "одного окна" и информатизации (Коробова А.Н.) в срок до 01.10.2008 обеспечить подключение к СМС информационных систем и ресурсов управ районов.
4. Установить, что автоматизированные системы инсталлируются на рабочих местах и серверном оборудовании префектуры и управ районов только после регистрации в СМС префектуры Зеленоградского административного округа г. Москвы.
5. Использовать данные востребованности информационных ресурсов из СМС для подготовки предложений по модернизации компьютерной техники префектуры и управ районов.
6. Утвердить Правила организации антивирусной защиты (приложение 2), Правила работы в сети Интернет (приложение 3), Положение по организации парольной защиты при работе на объектах информатизации Зеленоградского административного округа г. Москвы (приложение 4).
7. Утвердить план работ по повышению безопасности при обработке на компьютерах информации открытой и ДСП в префектуре Зеленоградского административного округа города Москвы на 2008 год (приложение 5).
8. Утвердить Регламент обслуживания Центра обработки данных префектуры (приложение 6).

9. Установить, что в управлениях, отделах и секторах префектуры ответственными за соблюдение Правил, установленных по п. 6, являются руководители соответствующих структурных подразделений.

10. Главам управ районов Матушкино-Савелки, Панфиловского, Крюково (Ласточкин В.П., Чеботарев А.В., Бодаданов Д.А.), руководителям муниципалитетов "Матушкино", "Савелки", "Старое Крюково", "Силино", "Крюково" (Дудов А.В., Соколова Л.Н., Чаброва И.А., Шестакова Г.Н., Путивцев А.В.):

10.1. Устранить замечания, выявленные в ходе проверки в октябре 2007 года, на следование правилам безопасности при обработке на компьютерах информации ДСП.

10.2. Обеспечить выполнение требований по п. 6.

11. Отделу службы "одного окна" и информатизации (Коробова А.Н.):

11.1. Организовать в срок до 01.04.2008 централизованное сетевое обновление программных продуктов, контроль лицензионной политики и соблюдения правил по п. 6 пользователями.

11.2. Ежеквартально докладывать о случаях нарушения правил по п. 6 на заседаниях рабочей группы по информационной безопасности.

11.3. В срок до 01.03.2008 произвести плановую замену паролей пользователей для доступа в операционную систему Windows и к автоматизированной информационной системе электронного документооборота префектуры с обеспечением возможности использования ключей e-token при наличии у пользователей.

11.4. Совместно с организациями, осуществляющими техническое и сервисное обслуживание соответствующих информационных систем префектуры и управ районов, в срок до 01.07.2009 обеспечить подключение СМС к системе мониторинга информационных систем города Москвы в соответствии с требованиями, утвержденными Управлением информатизации города Москвы.

12. Снять с контроля распоряжение префекта от 30.06.2006 N 686-рп как выполненное.

13. Отменить приложение 2 к распоряжению префекта N 120-рп от 04.02.2005, приложение 3 к распоряжению префекта N 686-рп от 30.06.2006.

14. Контроль выполнения настоящего распоряжения возложить на первого заместителя префекта А.И. Михальченкова.

О ходе выполнения распоряжения доложить префекту в срок до 01.10.2009.

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Профиль автоматизированного рабочего места префектуры для настройки через систему мониторинга событий, состояния и производительности серверных и пользовательских программно-аппаратных ресурсов префектуры

Базовое программное обеспечение:

- операционная система Windows XP;
- Internet Explorer;
- антивирусное обеспечение;
- офисное программное обеспечение (MS Word, MS Excel, MS Power Point);
- справочно-правовая система "КонсультантПлюс";
- "Lotus-Notes", включающий в себя электронную почту и модули ЕАСДОУ;
- система корпоративного пейджинга (Sametime, QIP, Skype - по требованию пользователя);
- Крипто-Про (в случае, если пользователь - владелец средств ЭЦП);
- Net-Security (в случае, если пользователь - владелец e-token).

Для регистраторов единой автоматизированной системы документационного обеспечения управления (ЕАС ДОУ) и АИС ЕРКТ:

- система поточного сканирования АИДИС.

Для сотрудников отдела финансирования, бухгалтерского учета и отчетности:

- система "Парус";
- система "Смета-2000".

Для сотрудников управления государственной службы и кадров:

- "Кадры государственной службы" <*>.

Для сотрудников управления потребительского рынка и услуг:

- информационная система СИОПР <*>.

Для сотрудников управления строительства, транспорта и землепользования:

- БД учета садоводов и огородников;
- Autodesk <*>.

{pre} ---------- <*> Данные позиции действительны для сотрудников, имеющих доступ к соответствующей программе. {/pre}

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Правила организации антивирусной защиты

Поставка антивирусных средств

Организацией антивирусной защиты занимается отдел службы "одного окна" и информатизации префектуры/службы администрирования управ и муниципалитетов.

Требования к использованию антивирусных средств

Антивирусными программами должен быть оснащен каждый компьютер органов исполнительной власти Зеленоградского административного округа г. Москвы. Запрещена установка бета-версий и версий с ограниченной функциональностью. После инсталляции программы конфигурируются в соответствии со следующими требованиями:

1. Загрузка антивируса должна выполняться автоматически при включении компьютера.
2. Антивирусное средство должно постоянно работать в фоновом режиме.
3. Не реже одного раза в неделю антивирусное ПО должно запускаться на сканирование всех жестких дисков.
4. Обязательна проверка исполняемых файлов (имеющих расширения .bat, .bin, .com, .dll, .exe, .sys и др.), файлов с данными приложений, содержащих мобильный код (с расширениями .doc, .dot, .rtf, .xls, .xlt и др.).
5. Должны проверяться все файлы, находящиеся на гибких дисках, в приложениях к письмам электронной почты, загружаемые из Интернета или находящиеся на любых других внешних устройствах, таких как ZIP- и USB-дисках и т.п.
6. При обнаружении вируса пользователь должен быть немедленно извещен об этом антивирусной программой.
7. Протокол проверки компьютера на вирусы необходимо хранить не менее 30 суток.

Порядок обновления антивирусных баз и реагирование на инциденты

Установить следующий режим обновления антивирусных средств и баз вирусов к ним:

1. Рекомендуемый период обновления - ежедневно, для изолированных компьютерных сетей и отдельных компьютеров - еженедельно.
2. Стандартный период обновления - не реже одного раза в неделю.
3. Предельный период обновления - 14 дней.

Информация обо всех случаях обнаружения вирусов передается в службу администрирования ОИВ, которая анализирует инцидент, оперативно разрабатывает в случае необходимости мероприятия по противодействию и обеспечивает своевременное уведомление ответственного за информационную безопасность соответствующего органа исполнительной власти Зеленограда.

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Правила пользования услугами передачи данных в мультисервисной сети органов исполнительной власти Зеленоградского административного округа г. Москвы и сети интернет

Общие положения

Настоящие Правила пользования услугами передачи данных в мультисервисной сети органов исполнительной власти Зеленоградского административного округа г. Москвы и сети Интернет (далее - Правила) обязательны для пользователя при использовании услуг передачи данных от электронного почтового ящика до каналов связи в мультисервисной сети органов исполнительной власти Зеленограда (далее - МС ОИВ Зеленограда).

В основу настоящих Правил положены общепринятые нормы работы в публичных компьютерных сетях, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Пользователь обязан соблюдать Правила использования информационного ресурса. Любые действия пользователя, нарушающие настоящие Правила пользования соответствующими информационными ресурсами, недопустимы.

Регистрация пользователей

Доступ в сеть Интернет из МС ОИВ Зеленограда предоставляется только зарегистрированным пользователям, не обрабатывающим информацию ограниченного пользования, в соответствии с приказом префекта от 09.12.2003 N 339-пп. Пользователь является зарегистрированным, если существует его учетная запись. Учетные записи для сотрудников подразделений префектуры создаются на основании приказа о приеме на работу от отдела кадров. При приеме на работу пользователю генерируется и передается пароль входа в операционную систему и МС ОИВ Зеленограда в соответствии с Положением по организации парольной защиты при работе на объектах информатизации префектуры и после ознакомления с настоящими Правилами.

Обязательства пользователя

При подключении к МС ОИВ Зеленограда пользователь принимает на себя обязательства:

1. Не отправлять по каналам МС ОИВ Зеленограда и сети Интернет информацию, которая противоречит законодательству Российской Федерации или законодательству города Москвы, а также международному законодательству.
2. Не использовать МС ОИВ Зеленограда и сеть Интернет для распространения материалов, оскорбляющих человеческое достоинство, пропагандирующих насилие или экстремизм, разжигающих расовую, национальную или религиозную вражду, преследующих хулиганские или мошеннические цели.
3. Не посылать, не публиковать, не передавать, не воспроизводить и не распространять любым способом программное обеспечение или другие материалы, полностью или частично защищенные авторскими или другими правами, без разрешения владельца или его полномочного представителя.
4. Не использовать МС ОИВ и сеть Интернет для распространения получателю незапрошенной информации (создания или участия в сетевом шуме - "спаме"), за исключением системных технических сообщений, санкционированных службой технической эксплуатации префектуры, управ районов. В частности, являются недопустимыми следующие действия:

- массовая рассылка предварительно не согласованных электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю. Под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств личного обмена информацией;
- рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения;
- использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных координат при совершении любого из

вышеописанных действий.

5. Не использовать идентификационные данные (имена, адреса, телефоны и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа).
6. Не фальсифицировать свой IP-адрес, адреса, используемые в других сетевых протоколах, а также прочую служебную информацию при передаче данных в МС ОИВ и сети Интернет.
7. Не производить без согласования с отделом службы "одного окна" и информатизации префектуры/службы администрирования соответствующего ОИВ установку дополнительного программного обеспечения и не изменять конфигурацию операционной системы компьютера, не вносить изменения в файлы, не принадлежащие самому пользователю.
8. Не разрабатывать и не распространять любые виды компьютерных вирусов.
9. Не использовать каналы связи МС ОИВ Зеленограда и сети Интернет для приема, передачи и записи файлов мультимедиа (видео, музыка, игры, графика), стороннего программного обеспечения, посещать ресурсы, не связанные с выполнением непосредственных служебных обязанностей пользователя. Проверка выполнения требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в МС ОИВ Зеленограда. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, обеспечивается службой администрирования МС ОИВ Зеленограда.
10. Не использовать каналы связи МС ОИВ Зеленограда для пропуска исходящего трафика от иных операторов и сетей связи.
11. Не осуществлять действия с целью изменения настроек оборудования или программного обеспечения или иные действия, которые могут повлечь за собой сбои в их работе.
12. Не осуществлять запуск приложений с непроверенных сайтов, из вложений в электронных письмах, пришедших от известных адресатов, а также не проверенных антивирусом внешних носителей.
13. Не осуществлять попытки несанкционированного доступа к информационным ресурсам сети, действия, направленные на нарушение нормального функционирования элементов МС ОИВ (компьютеров, маршрутизаторов, другого сетевого оборудования или программного обеспечения).

    При обнаружении попыток несанкционированного доступа, при подозрении на наличие вируса пользователь должен немедленно обратиться в отдел службы "одного окна" и информатизации префектуры или службу администрирования соответствующего органа исполнительной власти Зеленограда.

    Нарушение данных Правил влечет за собой лишение права пользования информационными ресурсами МС ОИВ и сети Интернет, а также наложение мер дисциплинарной ответственности в установленном порядке.

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Положение по организации парольной защиты при работе на объектах информатизации Зеленоградского административного округа г. Москвы

1. Общие положения

Аутентификация пользователей при работе на объектах информатизации префектуры Зеленоградского административного округа г. Москвы осуществляется с использованием индивидуальных паролей или специальных технических средств.

1.1. Настоящее Положение определяет порядок обеспечения защиты локальных автоматизированных систем (АС) и ПЭВМ, использующих подсистемы парольной защиты от несанкционированного доступа (НСД).

1.2. Парольная защита при работе на объекте информатизации осуществляется с целью предотвращения несанкционированного доступа к несекретной и с грифом "Для служебного пользования" информации (далее - несекретная информация), обрабатываемой в АС префектуры, управах районов и муниципалитетах Зеленоградского административного округа г. Москвы.

1.3. Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от НСД.

К основным видам (категориям) паролей относятся:

- пароли доступа к прикладным программам, обеспечивающим доступ к несекретной информации;
- пароль доступа средств защиты от НСД;
- пароли систем доступа встроенных в используемые операционные системы (ОС) серверного оборудования и АРМ пользователей.

1.4. Порядок работы с паролями вводится с момента утверждения данного Положения.

1.5. Данное Положение доводится до сведения сотрудников подразделений префектуры, управ районов и муниципалитетов под роспись.

2. Основные требования к организации парольной защиты

2.1. Личные пароли доступа к объекту информатизации, системе защиты от НСД вырабатываются автоматизированной системой генерации паролей администраторами ЛВС и информационными администраторами в рамках своей компетенции с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 или 1йфячыц2 и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 последовательных позициях;
- в числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- не использовать ранее присвоенные пароли одним и тем же пользователям;

- записи о паролях не должны храниться в непосредственной близости от АРМ.

2.2. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящего Положения и других руководящих документов по паролированию;
- своевременно сообщать ответственному за информационную безопасность о всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

2.3. При организации парольной защиты запрещается:

При использовании аутентификации при помощи пароля:

- записывать свои пароли в очевидных местах, таких как монитор, на системном блоке ПЭВМ, на обратной стороне клавиатуры и т.д.;
- хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги, доступных для посторонних лиц;
- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

При использовании аутентификации при помощи USB-ключа eToken:

- снимать несанкционированные копии с носителей ключевой информации;
- знакомить с содержанием носителей ключевой информации или передавать носители ключевой информации лицам, к ним не допущенным;
- выводить секретные ключи на дисплей (монитор) ПЭВМ или принтер;
- устанавливать носитель в считывающее устройство ПЭВМ, на которой программные средства передачи-приема функционируют в непредусмотренных (нештатных) режимах, а также на другие ПЭВМ;
- записывать на носители ключевой информации постороннюю информацию.

2.4. Руководители структурных подразделений несут персональную ответственность за организацию работ в подразделении по выполнению требований настоящего Положения и других документов, регламентирующих использование парольной защиты.

2.5. Ответственность за непосредственную работу с паролями (своевременный ввод в действие, замену и уничтожение) возлагается на уполномоченных лиц.

2.6. На подразделение, эксплуатирующее ПЭВМ, возлагаются следующие задачи:

- обеспечение руководства функционированием системы парольной защиты;
- контроль за реализацией требований по обеспечению безопасности при использовании паролей в АС.

3. Порядок применения парольной защиты

3.1. Полная плановая смена паролей в АС проводится регулярно, не реже одного раза год с ведением соответствующего журнала учета паролей.

3.2. Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя автоматизированной системы должна производиться в следующих случаях:

- по окончании срока действия;
- в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) пользователя ПЭВМ;
- по указанию ответственного за информационную безопасность или начальника первого отдела.

Примечание. При использовании ключа eToken для аутентификации в указанных случаях он подлежит сдаче ответственному по информационной безопасности префектуры с последующим обязательным выполнением процедуры персонификации для нового пользователя АРМ.

3.3. Смена пароля осуществляется ответственным за информационную безопасность.

3.4. Для предотвращения доступа к информации, находящейся в ПЭВМ, минуя ввод пароля, пользователь по окончании сеанса работы или во время перерыва в работе обязан осуществить выход из системы.

3.5. Пароли, используемые для локального доступа к программно-аппаратным средствам (ПАС) и доступа к ресурсам АС, вводятся пользователем с клавиатуры или с использованием ключа eToken для входа в систему.

3.6. Компрометация действующих паролей является нарушением системы информационной безопасности, о чем владелец пароля оперативно информирует ответственного за информационную безопасность и начальника первого отдела.

Под компрометацией понимаются хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия ответственного исполнителя, приведшие к получению его пароля лицами, не имеющими на то права.

3.7. Скомпрометированные пароли и ключи eToken выводятся из действия.

Порядок внеплановой смены аналогичен плановой смене паролей.

3.8. По каждому случаю, связанному с компрометацией действующих паролей, организуется и проводится в установленном порядке служебное расследование.

По результатам расследования к лицам, допустившим разглашение паролей, принимаются необходимые административные меры.

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

План работ по повышению безопасности при обработке на компьютерах информации открытой и дсп в префектуре Зеленоградского административного округа города Москвы на 2008 год

N п/п	Мероприятие	Срок исполнения
1.	Подготовить общую инструкцию пользователю по работе с ПК	Январь 2008 г.
2.	Разграничить права доступа к информации на местах пользователей: - к локальным файлам; - к сетевым ресурсам; - к ресурсам Интернет; - к системным настройкам; - ограничения доступа по IP-адресам	Январь 2008 г.
3.	Организовать работы по подключению и настройке ленточной библиотеки и системы хранения данных	Январь 2008 г.
4.	Провести замену паролей в серверной части префектуры	Январь - февраль 2008 г.
5.	Организовать учет всей компьютерной техники, в том числе техники, вышедшей из строя	Январь - февраль 2008 г.
6.	Организовать установку (с приоритетом для мест с обработкой информации для служебного пользования) необходимого программного обеспечения для входа в программную среду Windows с помощью аппаратных средств - электронных ключей e-token	Январь - февраль 2008 г.
7.	Наладить резервное копирование данных пользователей	Февраль 2008 г.
8.	Организовать работу системы массовых системных рассылок пользователям	Февраль 2008 г.
9.	Провести необходимые ежегодные мероприятия по смене паролей доступа к системе на местах пользователей с обеспечением возможности использования ключей e-token	Март 2008 г.
10.	Объединить компьютеры по группам и разбить группы по Vlan (в соответствии с утвержденной политикой общения между пользователями различных Vlan)	Март 2008 г.
11.	Установка и настройка Microsoft System Management Server (возможность мониторинга сервисов и аппаратного обеспечения)	Март 2008 г.
12.	Установка и настройка Microsoft Operations Manager (централизованное управление информационными системами)	Март 2008 г.
13.	Проведение плановых проверок пользователей на предмет соблюдения регламента по информационной безопасности	Март 2008 г.
14.	Организация централизованного сетевого обновления программных продуктов, контроль лицензионной политики и соблюдения правил работы в Интернете и обновления антивирусных программ	01.04.2008

15.	Проведение комплексного обследования СЗИ префектуры	II кв. 2008 г.
16.	Подключение с SMS и МОМ информационных ресурсов управ районов	01.10.2008
17.	Подготовка отчета в рабочий аппарат Комиссии по информационной безопасности при Мэре Москвы, информационной справки о выполнении мероприятий в сфере обеспечения информационной безопасности	До 01.10.2008
18.	Подготовка заявки в Первое управление г. Москвы по мероприятиям по повышению безопасности при обработке на компьютерах информации с грифом ДСП на 2009 год	Декабрь 2008 г.
19.	Закупка и установка модулей расширения межсетевого экрана Firewall	Декабрь 2008 г.
20.	Провести инвентаризацию руководств и инструкций, необходимых для эксплуатации и администрирования сети	Декабрь 2008 г.
21.	Проработка и заключение корпоративного лицензионного соглашения с Microsoft	В течение 2008 г.
22.	Закупка, установка и настройка дополнительно необходимых лицензионных продуктов и обновление существующих	В течение 2008 г.
23.	Своевременное обновление программного обеспечения и антивирусных баз: - Windows; - Антивирус "Касперского" (обновления на рабочих станциях должны производиться локально)	Постоянно в соответствии с Правилами антивирусной защиты и по мере поступления обновлений Windows
24.	Провести необходимые мероприятия по модернизации отдельных рабочих мест путем увеличения оперативной памяти	По мере необходимости в соответствии с данными СМС
25.	Контроль и анализ Интернет-трафика. Подготовка отчета и рассмотрение на заседании рабочей группы по информационной безопасности	Ежеквартально

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Регламент обслуживания центра обработки данных

Центр обработки данных (далее - ЦОД) построен в кабинете 227 префектуры Зеленоградского АО г. Москвы. ЦОД относится к помещениям с ограниченным доступом. ЦОД предназначен для обеспечения технических (энергетических, температурных) условий эксплуатации коммутирующего, серверного и телефонного оборудования префектуры и построен на базе интегрированного решения компании APC InfraStruXure.

1. Доступ в помещения ЦОД

1.1. В помещения ЦОД префектуры допускаются лица, которые имеют прямое отношение к ведущимся в этих помещениях работам. Перечень таких лиц утверждается руководителем аппарата префектуры. Доступ других лиц в серверные помещения префектуры может быть разрешен только в случае служебной необходимости руководителем аппарата префектуры, заместителем префекта по направлению или начальником отдела службы "одного окна" и информатизации.

1.2. Все работы, включая уборку и другие необходимые хозяйственные работы, в ЦОД могут проводиться только в присутствии лиц по п. 1.1.

1.3. Доступ в ЦОД осуществляется по индивидуальным магнитным картам, которые программируются администратором сети префектуры для доступа в ЦОД.

1.4. Доступ в ЦОД фиксируется в специальной программе с указанием Ф.И.О. владельца карты, даты и времени, идентификационных данных открытых помещений ЦОД, времени открытия коммуникационных шкафов ЦОД. Данные программы подлежат обязательному резервированию и хранению архива не менее чем год.

1.5. Все ключи от механических замков ЦОД хранятся в железном шкафу, находящемся в буферном помещении ЦОД. При этом механические замки в инженерное помещение и серверное помещение ЦОД являются нормально открытыми, магнитные замки - нормально закрытыми. Ключ от механического замка главной входной двери ЦОД хранится на посту охраны здания префектуры.

1.6. При индикации на пульте охраны здания префектуры о пожаре или аварии в помещении ЦОД дежурный по префектуре и работники охраны немедленно вызывают пожарную команду или аварийно-спасательную службу, вызывают начальника отдела службы "одного окна" и информатизации, ставят в известность префекта, его заместителя, курирующего информатизацию, и принимают меры к ликвидации пожара или аварии и спасению имущества ЦОД.

2. Состав оборудования ЦОД

Оборудование, размещенное в помещении ЦОД, по своему назначению делится на два класса:

- аппаратно-программные средства обеспечения работы ЦОД, входящие в состав интегрированного решения APC InfraStruXure:
- система охранной сигнализации;
- система пожарной сигнализации;
- система контроля и управления доступом;
- система автоматического газового пожаротушения;
- система кондиционирования помещения;
- система вентиляции и газоудаления;
- система электропитания, система основного и аварийного освещения;
- система бесперебойного электропитания;
- система управления и мониторинга телеметрией помещения и технических шкафов, система контроля доступа;
- аппаратно-программные средства, обеспечивающие работоспособность непосредственно сервисов служб

префектуры и округа:

- АПК телефонной сети (АТС Definity);
- АПК ЛВС (центральный коммутатор ЛВС);
- АПК служб и сервисов (серверы префектуры);
- кабельное хозяйство.

Подробное описание оборудования ЦОД приведено в техническом описании (ТО), исполнительской документации (ИО) ЦОД.

3. Система управления ЦОД

Система управления ЦОД является комплексом административных мер, обеспечивающих единый порядок (правила) эксплуатации ЦОД.

3.1. Непосредственная эксплуатация ЦОД осуществляется эксплуатирующей организацией, с которой собственник заключил государственный контракт на обслуживание ЦОД.

3.2. Собственник управляет работой ЦОД через уполномоченного представителя силами эксплуатирующей организации путем выдачи поручений (предписаний) в письменном виде с указанием срока исполнения, оригинал поручений подшивается в Журнал распоряжений и хранится в шкафу в ЦОД.

3.3. Эксплуатирующая организация обеспечивает соблюдение правил эксплуатации и сроков выполнения распоряжений собственника и регламентных работ.

3.4. Все виды работ, которые проводятся в ЦОД силами эксплуатирующей организации либо сторонними организациями по договорам с собственником, производятся в присутствии дежурного инженера эксплуатирующей организации с письменного разрешения собственника. О всех работах, проведенных в ЦОД, производится запись-отчет в Журнале регистрации изменений.

3.5. Перед выполнением работ на территории ЦОД инженерами эксплуатирующей организации либо инженерами сторонних организаций дежурный инженер эксплуатирующей организации проводит инструктаж по технике безопасности, о чем делается запись в Журнале инструктажа по ТБ.

3.5. Эксплуатирующая организация к концу срока действия действующего государственного контракта на эксплуатацию ЦОД сдает собственнику пакет технической документации со всеми внесенными изменениями в ходе эксплуатации ЦОД. Промежуточный надзор за соблюдением настоящего Регламента возлагается на уполномоченного представителя собственника и руководителя эксплуатирующей организации. Проверка соблюдения правил Регламента производится 1 раз в месяц, о чем делается запись в Журнале проверок.

4. Документация ЦОД

4.1. Документация ЦОД есть комплекс документов, в которых отражены принципы управления и обслуживания ЦОД.

4.2. Перечень обязательных документов ЦОД:

1. Структурная схема ЦОД и ЛВС формата 2 А1:1 крепится на стене операторской комнаты. Отображает структурное построение систем связи в здании.
2. Исполнительская документация на системы и подсистемы ЦОД:

- копии документов проектирующей организации.

3. Лицензионное программное обеспечение на систему APC InfraStruXure в виде компакт-дисков, описание на бумажных носителях:

- APC Symmetra PX XR Battery Enclosure (10-40 kW) - 1 шт.;
- APC Switched Rack Power Distribution Unit - 13 шт. + 12 CD;
- APC Environmental Manager System (AP9320) - 1 шт. + 1 CD;
- APC InfraStruXure Manager (ACRC100, ACRC101, ACRC102) - 6 шт. + 1 CD;
- APC NetShelter SX Enclosure (AR3100, AR3107, AR3150, AR3157) - 4 шт. + 3CD;
- APC Ethernet Switches (AP9224110, AP9224111, AP9224112) - 1 шт. + 1 CD;
- APC (инструкция по сборке шкафа) - 18 шт.;

- Carel (очиститель воздуха) - 4 шт.;
- SIGMA Water chiller - 1 шт.;
- Unilift - насос (CC5, CC7, CC9) - 1 шт.;
- Xchange cooler - 1 шт.

4. Лицензионное программное обеспечение на систему контроля доступа в виде компакт-дисков, описание на бумажных носителях.
5. Журнал проведения регламентных работ содержит точный перечень работ с указанием нормативов, порядка и сроков организации всех видов регламентных работ.
6. Журнал проверок содержит отметки о проведении проверок соблюдения Регламента.
7. Журнал инструктажа по ТБ содержит отметки о проведении инструктажа по ТБ.
8. Журнал регистрации изменений содержит отметки о проведении изменений в схему связи.
9. Журнал распоряжений содержит поручения собственника ЦОД - основания для произведения изменений в настройках ЦОД.
10. Журнал системы информационной безопасности отображает построенную систему безопасности, реализованные права доступа пользователей, производятся отметки об изменениях системы безопасности.
11. Журнал должностных инструкций - в данном журнале содержатся инструкции должностных лиц, ответственных за эксплуатацию ЦОД, с отметками об ознакомлении:

- список должностных лиц, ответственных за эксплуатацию ЦОД, контакты и приоритет извещения;
- инструкция руководителя эксплуатирующей организации;
- инструкция главного инженера;
- инструкция дежурного инженера;
- инструкция оператора;
- инструкция о действиях при пожаре;
- инструкция о действиях в аварийных ситуациях;
- перечень, формы документов, правила заполнения документов, регламентирующих работу ЦОД.

5. Система обозначений оборудования ЦОД

5.1. Система обозначений ЦОД основана на исполнительской документации и реализуется в шкафах ЦОД и служебной документации.

5.2. Каждый шкаф в ЦОД дополнен листом адресной документации, который является техническим паспортом шкафа.

5.3. Технический паспорт шкафа ЦОД должен отражать информацию об установленном в шкафу оборудовании, технических параметрах, реализованных на базе установленного оборудования сервисах, входящих и исходящих соединениях оборудования, сроках гарантии на оборудование, название и контактные данные организации, ответственной за гарантийное обслуживание.

5.4. Технический паспорт шкафа, расположенного в ЦОД и в котором установлено оборудование сторонних операторов связи, должен отражать информацию об установленном в шкафу оборудовании, реализованных услугах, входящих и исходящих соединениях оборудования, контактные данные организации, ответственной за эксплуатацию установленного оборудования.

6. Регламентные работы в ЦОД

6.1. Регламентные работы, проводимые на оборудовании ЦОД, делятся на:

- еженедельные;
- ежемесячные;
- полугодовые.

6.2. Еженедельные регламентные работы производятся силами дежурного инженера эксплуатирующей

организации в назначенный день в рабочее время менее без выключения оборудования.

Виды работ:

- замена и удаление патчкордов;
- замена неисправных модулей и корпусов;
- контроль параметров электропитания;
- состояния ИБП;
- работоспособность системы климат-контроля.

Виды работ по аппаратно-программной части серверов: в соответствии с приложением 6.

6.3. Ежемесячные регламентные работы проводятся инженерами эксплуатирующей организации под руководством администратора системы и выполняются в рабочее и нерабочее время. Выключение серверов и коммутаторов производится только в нерабочее время.

Виды работ:

- уборка в шкафах, удаление пыли с защитных сеток вентиляторов модулей питания;
- замена и удаление патчкордов;
- замена неисправных модулей и корпусов;
- контроль параметров электропитания;
- состояния ИБП;
- работоспособность системы климат-контроля.

Виды работ по аппаратно-программной части серверов: в соответствии с приложением 6.

6.4. Полугодовые регламентные работы проводятся инженерами эксплуатирующей организации под руководством администратора либо главного инженера с привлечением инженеров представителей организаций, несущих гарантийные обязательства на оборудование. Полугодовые регламентные работы производятся в выходные и рабочие дни с письменным извещением собственника.

Виды работ:

- контроль параметров и обслуживание систем климат-контроля;
- контроль параметров и обслуживание системы пожаротушения;
- тестирование системы автоматического подключения резервного питания;
- замена неисправного оборудования.

Виды работ по аппаратно-программной части серверов: в соответствии с приложением 6.

Во время проведения полугодовых регламентных работ отключение питания серверов и коммутаторов допускается только в нерабочее время.

6.5. Все виды регламентных работ производятся в строгом соответствии с паспортными данными на устройства, подлежащие обслуживанию.

7. Действия при аварийных ситуациях в ЦОД

7.1. В случае аварийной ситуации система оповещения APC InfraStruXure автоматически направляет SMS на телефоны дежурной службы эксплуатирующей организации и дежурной службы собственника.

7.2. В случае получения сообщения об аварийной ситуации дежурный инженер эксплуатирующей организации обязан прибыть в ЦОД в рабочее время немедленно, в нерабочее время - не позднее чем через 30 мин. после получения сообщения об аварии. Дежурный инженер, прибывший на место, принимает меры к устранению аварийной ситуации в соответствии с должностной инструкцией и особенностями аварии, о принятом решении и результатах сообщает дежурной службе собственника и руководителям, приведенным в списке должностных лиц, ответственных за эксплуатацию ЦОД.

7.3. После устранения аварийной ситуации дежурный инженер делает запись-отчет в Журнале регламентных работ в разделе "Отчет о сбоях Журнала проведения регламентных работ". Информация об аварии

передается начальнику отдела службы "одного окна" и информатизации. В случае аварии на оборудовании, стоящем на гарантийном обслуживании, на основе отчета о сбоях направляется письменное уведомление в организацию, несущую гарантийные обязательства, на следующий рабочий день после совершения аварии.

8. Охрана труда

8.1. Общие положения.

8.1.1. Руководящими документами для организации охраны труда на предприятии, эксплуатирующем ЦОД префектуры Зеленоградского АО г. Москвы, являются:

- основные положения действующего законодательства Российской Федерации об охране труда;
- приказ Минсвязи России от 02.09.93 N 207.

8.1.2. Организация охраны при выполнении работ в ЦОД есть комплекс административно-технических мер, соблюдаемых всеми категориями работников предприятия с целью сохранения жизни и здоровья людей, а также соблюдение правил и норм обслуживания оборудования, гарантирующего исправность узлов и агрегатов, и выполнение задач, возложенных на ЦОД.

8.1.3. Основой правильных действий при выполнении работ является знание всеми категориями работников и руководителей своих функциональных обязанностей в части выполнения их на территории ЦОД, а также знание и неукоснительное соблюдение требований техники безопасности при работе в ЦОД и знание инструктажа по ТБ перед выполнением работ.

8.2. Организация охраны труда в ЦОД префектуры Зеленоградского АО г. Москвы.

8.2.1. Инструктаж по технике безопасности.

По характеру и времени проведения инструктажи подразделяют:

1. Вводный.
2. Первичный на рабочем месте.
3. Повторный.
4. Внеочередной.
5. Целевой.

8.2.1.1. Примерный перечень вопросов вводного инструктажа.

1. Общие сведения о предприятии, учреждении, организации, характерные особенности производства.
2. Основные положения законодательства об охране труда.

2.1. Трудовой договор (контракт).

2.2. Рабочее время и время отдыха.

2.3. Охрана труда женщин.

2.4. Охрана труда молодежи.

2.5. Льготы и компенсации за работы с вредными условиями труда.

2.6. Правила внутреннего трудового распорядка предприятия, учреждения, организации, ответственность за нарушение правил.

2.7. Организация работы по охране труда на предприятии. Ведомственный, государственный надзор и общественный контроль за состоянием охраны труда.

3. Общие правила поведения работающих на территории предприятия, в производственных и вспомогательных помещениях, в местах проведения работ на обслуживаемых участках. Расположение основных производственных зданий и сооружений, цехов, служб, вспомогательных помещений.

8.2.2.1. Примерный перечень вопросов первичного инструктажа на рабочем месте.

1. Общие сведения о технологическом процессе и оборудовании на данном рабочем месте, производственном участке, в цехе. Основные опасные и вредные производственные факторы, возникающие при данном технологическом процессе.

2. Безопасная организация и содержание рабочего места.

3. Опасные зоны машины, механизма, прибора. Средства безопасности оборудования (предохранительные, тормозные устройства и ограждения, системы блокировки и сигнализации, знаки безопасности). Требования по предупреждению электротравматизма.

4. Порядок подготовки к работе (проверка исправности оборудования, пусковых приборов, инструмента и приспособлений, блокировок, заземления и других средств защиты).

5. Безопасные приемы и методы работы; действия при возникновении опасных ситуаций.

6. Средства индивидуальной защиты на данном рабочем месте и правила пользования ими.

7. Схема безопасного передвижения работающих на территории ЦОД.

8. Требования безопасности при погрузочно-разгрузочных работах и транспортировке грузов.

9. Характерные причины аварий, взрывов, пожаров, случаев производственных травм.

10. Меры предупреждения аварий, взрывов, пожаров. Обязанность и действия при аварии, взрыве, пожаре. Способы применения имеющихся на участке средств пожаротушения, противоаварийной защиты и сигнализации, места их расположения.

8.2.3.1. Внеочередной инструктаж.

Внеочередной инструктаж проводят:

- при введении в действие новых или переработанных стандартов, правил, инструкций по охране труда, а также изменений к ним;

- при изменении технологического процесса, замене или модернизации оборудования, приспособлений и инструмента, исходного сырья, материалов и других факторов, влияющих на безопасность труда;

- при нарушениях работающими требований безопасности труда, которые могут привести или привели к травме, аварии, взрыву или пожару, отравлению;

- по требованию органов надзора.

8.3. Порядок проведения инструктажа по ТБ и ответственные лица.

8.3.1. Ответственным за организацию ТБ при выполнении работ по системам связи является руководитель эксплуатирующей организации. Ответственным за соблюдение правил ТБ на территории ЦОД является дежурный инженер.

8.3.2. Все работы в ЦОД проводятся в сопровождении дежурного инженера эксплуатирующей организации либо им самим в сопровождении помощника. Запрещено производить какие-либо работы на территории ЦОД количеством человек менее 2.

Работа на территории ЦОД производится по следующим этапам:

начало работ - инструктаж по ТБ с обязательной отметкой в Журнале инструктажа по ТБ;

проведение работ на системах и оборудовании;

оформление документации по итогам проведения работ.

8.3.3. Оригинальный текст Инструкции по ТБ работы в ЦОД, Инструкции по действиям в аварийных ситуациях приведен в приложении 1, должен быть прикреплен на двери ЦОД изнутри и двери комнаты оператора.

9. Взаимодействие операторов связи и держателей оборудования в ЦОД

9.1. Размещение оборудования, технических средств в ЦОД должно соответствовать правилам техники безопасности, санитарным нормам и отвечать требованиям пожарной безопасности.

9.2. Действия по размещению, перемещению или удалению какого-либо оборудования в ЦОД производятся на основании письменного указания представителя собственника ЦОД.

9.3. В случае принятия решения собственником ЦОД о размещении дополнительного оборудования в шкафах ЦОД, принадлежащего собственнику либо сторонней организации, подключении к оборудованию ЦОД дополнительных каналов связи необходимы подготовка проекта и его согласование со службой эксплуатации здания и отделом службы "одного окна" и информатизации префектуры.

9.4. Основанием для размещения оборудования в шкафах ЦОД служит указание представителя собственника в

письменном виде с присутствующими согласующими подписями уполномоченных специалистов. А также документ - указание о предоставлении оборудованию (информационному ресурсу) статуса приоритета в системе безопасности за подписью начальника отдела службы "одного окна" и информатизации префектуры.

9.5. В случае необходимости проведения каких-либо работ на оборудовании ЦОД сторонними специалистами (специалистами операторов связи поставщиков услуг связи) основанием для допуска их к работам на территории ЦОД является письменное указание представителя собственника с указанием даты, времени, количества людей и видов работ.

9.6. Все работы на территории ЦОД выполняются в присутствии дежурного инженера эксплуатирующей организации.

10. Надзор за исполнением Регламента обслуживания ЦОД

10.1. Надзор за исполнением Регламента обслуживания ЦОД возлагается на руководителя эксплуатирующей организации и начальника отдела службы "одного окна" и информатизации, а также начальника сектора эксплуатации зданий префектуры.

10.2. Комплексная проверка выполняется должностными лицами не реже чем 1 раз в месяц с проверкой соблюдения всех пунктов настоящего Регламента. О каждой проверке делается запись в Журнале проверок с указанием даты, времени и объема проверенного Регламента.

10.3. Правом проверки исполнения Регламента наделяются руководители - должностные лица, утвержденные руководителем аппарата префектуры.

10.4. Журнал проверок хранится на территории ЦОД в металлическом ящике и действует в течение календарного года. По истечении календарного года Журнал проверок сдается в архив в качестве приложения к государственному контракту на обслуживание ЦОД.

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Инструкция руководителя эксплуатирующей организации

Руководитель эксплуатирующей организации является главным представителем предприятия (эксплуатирующей организации) исполнителя во всех мероприятиях, касающихся организации работы систем связи заказчика, и гарантом качества обслуживания по предмету государственного контракта.

Руководитель ЭО обязан:

1. Организовать работы по поддержанию систем и оборудования ЦОД, а также взаимодействие со сторонними операторами связи в соответствии с условиями государственного контракта, заключенного между эксплуатирующей организацией и государственным заказчиком, и на основании Регламента обслуживания ЦОД и настоящей инструкцией.
2. Осуществлять функции проверяющего при проверках соблюдения правил эксплуатации ЦОД в соответствии с Регламентом обслуживания ЦОД, о чем делает запись в Журнале проверок.
3. Организовать мероприятия по охране труда на территории ЦОД в соответствии с действующим законодательством и положениями Регламента обслуживания ЦОД.
4. Организовать мероприятия по технике безопасности при проведении работ в ЦОД на оборудовании и в сетях, подлежащих обслуживанию по предмету государственного контракта.
5. Организовать документальное сопровождение работ в соответствии с требованиями положений Регламента обслуживания ЦОД.

Инструкция главного инженера

Главный инженер ЭО назначается приказом руководства ЭО, является главным специалистом по организации работы систем и оборудования, приведенного в приложении к государственному контракту (Перечень оборудования, подлежащего обслуживанию по предмету государственного контракта, размещенного на территории ЦОД и других технических платформах заказчика).

Главный инженер ЭО обязан лично управлять системами связи по государственному контракту.

Главный инженер ЭО обязан лично организовать мероприятия по поддержанию в рабочем состоянии системы связи по государственному контракту.

Главный инженер ЭО участвует в выработке стратегии развития систем связи и информационных ресурсов, размещаемых на территории ЦОД и ЛВС, обслуживаемых по государственному контракту.

При проведении работ на территории ЦОД и в сетях связи заказчика главный инженер ЭО обязан организовать соблюдение мероприятий техники безопасности и охраны труда.

Главный инженер ЭО обязан проверять соблюдение правил Регламента обслуживания ЦОД и правил документального сопровождения работ.

Инструкция администратора ЦОД (дежурного инженера)

1. Общие положения

1.1. Администратор ЦОД префектуры Зеленоградского АО г. Москвы является специалистом по обслуживанию систем, размещенных на территории ЦОД.

1.2. Администратор ЦОД обязан проводить все работы на оборудовании ЦОД в соответствии с настоящим Регламентом и инструкцией администратору ЦОД. После окончания плановых или внеплановых работ администратор вносит запись в соответствующий журнал.

1.3. Администратор ЦОД обязан вести техническую документацию ЦОД.

1.4. Администратор ЦОД обязан следить за целевым использованием помещения ЦОД, не допуская присутствия либо хранения какого-либо оборудования и вещей, не связанных с работой ЦОД. Запрещено перемещение оборудования либо другого имущества по территории ЦОД без письменного разрешения (указания) лиц,

утвержденных руководителем аппарата префектуры.

1.5. Работы на территории ЦОД начинаются с инструктажа по технике безопасности, о чем делается запись в Журнале по ТБ.

1.6. Каждая единица оборудования, установленного в ЦОД, обслуживается в соответствии с положениями и правилами, приведенными в Регламенте. При организации работ по ТО администратор руководствуется требованиями настоящего Регламента.

1.7. В случае привлечения специалистов сторонних организаций для выполнения каких-либо работ администратор ЦОД присутствует лично на территории ЦОД во время выполнения работ и обеспечивает контроль работы ЦОН. Запрещено допускать либо оставлять на территории ЦОД специалистов, не имеющих допуск.

1.8. В соответствии с требованиями технической безопасности все работы, связанные с коммутацией, переносом, физическим включением и выключением оборудования ЦОД, выполняются составом не менее двух человек. Запрещено производить работы по физической коммутации оборудования самостоятельно.

2. Инструкция о действиях при пожаре

2.1. В целях предотвращения пожароопасных ситуаций на территории ЦОД запрещено приносить взрывчатые и горючие вещества. Запрещено курение и разведение огня. Запрещено принятие пищи.

2.2. Для обеспечения эффективных решений при работе на территории ЦОД и срабатывания охранно-пожарной сигнализации все категории работников обязаны изучить алгоритм работы программы управления системы охранно-пожарной сигнализации и системы пожаротушения.

2.3. В случае срабатывания охранно-пожарной сигнализации устройство "Odemco", смонтированное на стене в помещении оператора, разблокирует двери для того, чтобы дать возможность персоналу покинуть помещение - место возгорания. Через 30 сек. автоматически срабатывает система газового пожаротушения. Газ, вытесняющий кислород, подается с потолка и из-под фальшпола.

2.4. В случае если в момент возгорания на территории ЦОД остались люди, которые не могут самостоятельно покинуть помещение ЦОД по причине травмы либо ранения, сопровождающему инженеру необходимо принять меры к удалению людей и предотвращению поражения газом либо кислородной недостаточностью. Для этого дежурный инженер проникает в помещение ЦОД, надевает противогаз, установленный на стене слева от входа, второй противогаз надевает на пораженного и выводит из зоны тушения пожара.

2.5. После тушения пожара аппаратура системы газового пожаротушения открывает люки вентилятора, установленного вне помещения ЦОД, для вентиляции. Вход после пожаротушения для человека - не ранее чем через 30 минут принудительной вентиляции помещения.

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Журнал системы информационной безопасности

1. Настоящий Журнал заполняется дежурным инженером (администратором ЦОД) при выдаче/аннулировании паролей и прав доступа к ресурсам.
2. Основанием для выдачи/предоставления прав доступа к информационным ресурсам ЦОД является указание/распоряжение уполномоченного представителя собственника ЦОД в письменном виде.
3. Все документы с указанием/распоряжением уполномоченного представителя собственника ЦОД о предоставлении доступа к ресурсам подшиваются в настоящий Журнал.
4. При получении указания/распоряжения об изменении доступа к ресурсам дежурный инженер (администратор ЦОД) производит необходимые настройки, о чем делает запись с описанием произведенных работ в таблицу.

N	Дата	Основание. Ф.И.О. должностного лица, подписавшего документ	Суть произведенных изменений	Подпись исполнителя

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Правила ведения Журнала

1. Общие положения

1.1. Настоящий Журнал заполняется дежурным инженером (администратором ЦОД), а также руководителями, производящими инструктаж по ТБ при работе в ЦОД.

1.2. Инструктаж по технике безопасности.

По характеру и времени проведения инструктажи подразделяют:

1.2.1. Вводный.

1.2.2. Первичный на рабочем месте.

1.2.3. Повторный.

1.2.4. Внеочередной.

1.2.5. Целевой.

1.3. Примерный перечень вопросов вводного инструктажа.

1.3.1. Общие сведения о предприятии, учреждении, организации, характерные особенности производства.

1.3.2. Основные положения законодательства об охране труда.

1.3.2.1. Трудовой договор (контракт).

1.3.2.2. Рабочее время и время отдыха.

1.3.2.3. Охрана труда женщин.

1.3.2.4. Охрана труда молодежи.

1.3.2.5. Льготы и компенсации за работы с вредными условиями труда.

1.3.2.6. Правила внутреннего трудового распорядка предприятия, учреждения, организации, ответственность за нарушение правил.

1.3.2.7. Организация работы по охране труда на предприятии.

Ведомственный, государственный надзор и общественный контроль за состоянием охраны труда.

1.3.3. Общие правила поведения работающих на территории предприятия, в производственных и вспомогательных помещениях, в местах проведения работ на обслуживаемых участках.

1.4. Примерный перечень вопросов первичного инструктажа на рабочем месте.

1.4.1. Общие сведения о технологическом процессе и оборудовании на данном рабочем месте. Основные опасные и вредные производственные факторы, возникающие при данном технологическом процессе.

1.4.2. Безопасная организация и содержание рабочего места.

1.4.3. Опасные зоны машины, механизма, прибора. Средства безопасности оборудования (предохранительные, тормозные устройства и ограждения, системы блокировки и сигнализации, знаки безопасности). Требования по предупреждению электротравматизма.

1.4.4. Порядок подготовки к работе (проверка исправности оборудования, пусковых приборов, инструмента и приспособлений, блокировок, заземления и других средств защиты).

1.4.5. Безопасные приемы и методы работы; действия при возникновении опасных ситуаций.

1.4.6. Средства индивидуальной защиты на данном рабочем месте и правила пользования ими.

1.4.7. Схема безопасного передвижения работающих на территории ЦОД.

1.4.8. Требования безопасности при погрузочно-разгрузочных работах и транспортировке грузов.

1.4.9. Характерные причины аварий, взрывов, пожаров, случаев производственных травм.

1.4.10. Меры предупреждения аварий, взрывов, пожаров. Обязанность и действия при аварии, взрыве, пожаре. Способы применения имеющихся на участке средств пожаротушения, противоаварийной защиты и сигнализации, места их расположения.

1.5. Внеочередной инструктаж.

Внеочередной инструктаж проводят:

- при введении в действие новых или переработанных стандартов, правил, инструкций по охране труда, а также изменений к ним;
- при изменении технологического процесса, замене или модернизации оборудования, приспособлений и инструмента, исходного сырья, материалов и других факторов, влияющих на безопасность труда;
- при нарушениях работающими требований безопасности труда, которые могут привести или привели к травме, аварии, взрыву или пожару, отравлению;
- по требованию органов надзора.

1.6. Порядок проведения инструктажа по ТБ и ответственные лица.

1.6.1. Ответственным за организацию ТБ при выполнении работ по системам связи является руководитель эксплуатирующей организации. Ответственным за соблюдение правил ТБ на территории ЦОД является дежурный инженер.

1.6.2. Все работы в ЦОД проводятся в сопровождении дежурного инженера эксплуатирующей организации либо им самим в сопровождении помощника. Запрещено производить какие-либо работы на территории ЦОД количеством человек менее 2.

Работа на территории ЦОД производится по следующим этапам:

начало работ - инструктаж по ТБ с обязательной отметкой в Журнале инструктажа по ТБ;

проведение работ на системах и оборудовании;

оформление документации по итогам проведения работ.

1.7. Оригинальный текст Инструкции по ТБ работы в ЦОД, Инструкции по действиям в аварийных ситуациях приведен в приложении 1 и должен быть прикреплен на двери ЦОД изнутри и двери комнаты оператора.

1	Дата инструктажа	Ф.И.О., подпись инструктора	Тема инструктажа	Ф.И.О., подпись получившего инструктаж

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Правила ведения Журнала

1. Общие положения 1.3. Настоящий Журнал заполняется дежурным инженером (администратором ЦОД) при получении письменного указания от представителя собственника ЦОД о произведении необходимых изменений в настройках обслуживаемого оборудования.

1.4. Каждое произведенное изменение в настройках пользователей либо оборудования фиксируется с заполнением всех полей таблицы изменений и подписью исполнителя.

1.5. Документ - основание для произведения изменений в настройках оборудования ЦОД подшивается к настоящему Журналу.

1.6. Изменения, полученные от руководителя либо главного инженера эксплуатирующей организации, отображаются в общей таблице с заполнением всех полей таблицы.

1.7. Изменения, произведенные в системе связи ЦОД, одновременно отображаются на Структурной схеме связи ЦОД, прикрепленной к стене.

ТАБЛИЦА ВНЕСЕННЫХ ИЗМЕНЕНИЙ В НАСТРОЙКИ И СХЕМУ СВЯЗИ ОБОРУДОВАНИЯ ЦОД

N	Дата изменения, дата	Основание (документ с указанием Ф.И.О. распорядившегося)	Оборудование (номер и наименование оборудования по Структурной схеме связи ЦОД)	Суть произведенных изменений	Исполнитель. Подпись

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Правила ведения Журнала

1. Общие положения

1. Настоящий Журнал заполняется уполномоченными руководителями, приведенными в списке руководителей, ответственных за эксплуатацию ЦОД.

2. Периодичность проведения проверок устанавливается для мероприятий:

- ТО-1 - не реже 1 раза в неделю;

- ТО-2 - не реже 1 раза в месяц;

- ТО-3 - не реже 1 раза в 6 месяцев.

3. Руководитель, производящий проверку, делает запись о времени и объеме проверки в настоящем Журнале с указанием замечаний и рекомендациями и сроками устранения замечаний.

4. Дежурный инженер (администратор ЦОД) принимает меры к устранению замечаний по обслуживанию ЦОД в соответствии с установленными сроками. После устранения замечаний делает запись об устранении.

ОТЧЕТ О ПРОИЗВЕДЕННЫХ ПРОВЕРКАХ

N	Вид проверки	Замечания, рекомендации	Дата/подпись проверяющего	Дата/подпись исполнителя
	Произведена проверка проведения ТО-1 на сервере N 3		Подпись проверяющего	

Приложение
к Распоряжению от 18 января 2008 года № 22-рп

Правила ведения Журнала

1. Общие положения

1.1. Настоящий Журнал содержит точный перечень работ с указанием нормативов, порядка и сроков организации всех видов регламентных работ, проводимых на установленном в ЦОД оборудовании.

1.2. Установленное на территории ЦОД оборудование обслуживается в объеме, указанном в паспорте устройства, программы и на основании нормативных документов на обслуживание информационных ресурсов г. Москвы и договоров с эксплуатирующими организациями.

2. Ведение Журнала

2.1. В настоящем Журнале приведен список установленного на территории ЦОД оборудования с указанием объемов регламентных работ и периодичностью.

2.2. Дежурный инженер проводит работы по обслуживанию оборудования ЦОД на основе настоящего Журнала с указанной периодичностью и объемом работ.

2.3. После проведения регламентных работ ответственный инженер делает запись о выполненных работах с указанием индекса объема работ.

2.4. В связи с периодичностью выполняемым работам присваиваются следующие индексы:

еженедельное ТО - индекс "1";

ежемесячное ТО - индекс "2";

полугодовое ТО - индекс "3".

ОБЪЕМ РАБОТ ДЛЯ АППАРАТНОЙ И ПРОГРАММНОЙ ЧАСТИ ЦОД

	Наименование оборудования	ТО-1	ТО-2	ТО-3
	Обслуживаемое и необслуживаемое оборудование, установленное в ЦОД	Влажная уборка, пылесос; просмотр лог-файлов на наличие ошибок сетевых карт, оперативной памяти, жестких дисков, наличие свободного пространства, работоспособность информационной шины, тестирование всех аппаратных устройств в составе аппаратной платформы на соблюдение теплового режима	Проверка фильтров, теплообменника, увлажнителя и работы устройства. Визуальная проверка уровня хладагента. Визуальная проверка утечки хладагента. Проверка работы системы удаления конденсата. Проверка температуры охлаждающей воды Проверка чистоты внешнего теплообменника, очистка при необходимости. Проверка возможности изменения установок	Распечатываются отчеты по работоспособности аппаратной части. Производится замена неисправного пассивного оборудования в шкафах. Производится обслуживание оборудования, установленного в шкафах сторонних операторов, с привлечением специалистов. Тестирование систем пожаротушения охранно-пожарной сигнализации

			температуры и влажности. Проверка напряжения и питания. Проверка Журнала событий	

ОТЧЕТ О ПРОВЕДЕНИИ РЕГЛАМЕНТНЫХ РАБОТ ПО АППАРАТНОЙ ЧАСТИ ЦОД

N	Наименование оборудования	Дата проведения, объем, подпись									

ОТЧЕТ О ПРОВЕДЕНИИ РЕГЛАМЕНТНЫХ РАБОТ ПО ПРОГРАММНОЙ ЧАСТИ ЦОД

N	Наименование оборудования	Дата проведения, объем, подпись									