«УТВЕРЖДАЮ»
Директор ГБУ СО МО ЦСО
«Серпуховский городской дом ветеранов»
_____ С.В.Задорожнюк
«___» _____ 2011 г.

ПОЛОЖЕНИЕ
О РАЗРЕШИТЕЛЬНОЙ СИСТЕМЕ ДОПУСКА ИСПОЛНИТЕЛЕЙ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Настоящее Положение о разрешительной системе допуска исполнителей к конфиденциальной информации в ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» (далее – Положение) устанавливает единую разрешительную систему допуска к конфиденциальной информации в ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» (далее – Учреждение).

Положение не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

1.2. Конфиденциальная информация – это документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Сведения, относящиеся к конфиденциальной информации, определяются на основании Перечня сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера», и Постановления Правительства Московской области от 27 ноября 2002 г. № 573/46 «Об утверждении положения о порядке обращения с конфиденциальной информацией в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждениях Московской области».

1.3 К конфиденциальной информации относятся служебные сведения, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна). Порядок обращения с такого рода информацией определяется в соответствии с постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

На документах, содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

1.4. В соответствии с документами, перечисленными в п.1.2 настоящего Положения, в Учреждении разрабатывается «Перечень сведений конфиденциального характера ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов»».

2. ДОПУСК К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ УЧРЕЖДЕНИЯ

2.1. Допуск к конфиденциальной информации Учрежедния регламентируется действующим законодательством, а также настоящим Положением.

2.2. Руководители подразделений Учреждения (далее – руководители подразделений Учреждения) допускаются к конфиденциальной информации в объеме, необходимом для выполнения задач, стоящих перед подразделениями Учреждения (далее – подразделения Учреждения). Объем необходимой информации определяется директором ГБУ СО МО ЦСО

«Серпуховский городской дом ветеранов» (далее – директор) и заместителем директора по безопасности и АХЧ.

2.3. Допуск сотрудников Учреждения (далее – сотрудников Учреждения) к конфиденциальной информации осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими своих должностных обязанностей. Объем необходимой конфиденциальной информации определяет руководитель подразделения Учреждения.

2.4. Технический и обслуживающий персонал подразделений Учреждения допускается к конфиденциальной информации в объеме, необходимом для функционирования обслуживаемых технических средств и программных продуктов. Объем необходимой информации определяет руководитель подразделения Учреждения.

2.5. Все сотрудника Учреждения, допущенные к работе с конфиденциальной информацией, должны быть ознакомлены с Постановлением Правительства Московской области от 27 ноября 2002 г. № 573/46 «Об утверждении положения о порядке обращения с конфиденциальной информацией в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждениях Московской области» и с «Перечнем сведений конфиденциального характера Министерства», а также с обязанностями по ее сохранности и ответственностью в случае ее разглашения (ст.17 Федерального закона РФ от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации») Данный факт подтверждается личной подписью служащего в соответствующем журнале.

2.6. Допуск (предоставление информации) сторонних организаций к конфиденциальной информации Учреждения

2.6.1. Допуск (предоставление информации) сторонних организаций к конфиденциальной информации Учреждения регламентируется Постановлением Правительства Московской области от 27 ноября 2002 г. № 573/46 «Об утверждении положения о порядке обращения с конфиденциальной информацией в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждениях Московской области», а также настоящим Положением.

2.6.2. Допуск (предоставление информации) сторонним организациям осуществляется на основании действующих нормативно-правовых актов в соответствии:

- с разовым запросом;
- с официальным соглашением об обмене конфиденциальной информацией.

2.6.3. Для допуска (предоставления информации) по разовым запросам необходим письменный запрос, в котором указывается:

- для каких целей необходима информация;
- ее конкретное наименование.

2.6.4. Основанием для допуска (предоставления информации) служит резолюция директора.

2.6.5. Предоставление (передача) конфиденциальной информации осуществляется на бумажных и при необходимости, на иных носителях.

3. ПОРЯДОК ОФОРМЛЕНИЯ ДОПУСКА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СОТРУДНИКОВ УЧРЕЖДЕНИЯ

3.1. В соответствии с должностными обязанностями сотрудников Учреждения, на основании «Перечня конфиденциальной информации ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов»» и «Перечня защищаемых в Учреждении информационных ресурсов», директор определяет сотрудников Учреждения, которых необходимо допустить к конфиденциальной информации или информационным ресурсам автоматизированной системы (далее - АС) Учреждения.

3.2. Необходимость допуска сотрудника Учреждения к конкретной группе конфиденциальной информации отражается в заявке руководителя подразделения Учреждения на имя директора.

3.3. Допуск сотрудника Учреждения к конфиденциальной информации, непосредственно не связанной с выполнением его служебных обязанностей, должен быть обоснован руководителем подразделения в заявке, в которой указывается цель ознакомления и время, в течение которого сотрудник Учреждения допускается к информации.

3.4. Необходимость допуска сотрудника Учреждения к информационным ресурсам АС (в том числе и подлежащим защите), отражается руководителем подразделения Учреждения в заявке (Приложение № 1) на имя директора ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» , в которой определяются права и полномочия сотрудника.

Права сотрудника Учреждения определяют, к каким конкретно информационным ресурсам (программы, файлы, массивы, архивы, базы данных и т.п.) допускается конкретный сотрудник. Полномочия сотрудника Учреждения определяют, что конкретно (читать, изменять, удалять, копировать, печатать и т.п.) может делать допущенный к информационным ресурсам служащий.

3.5. На основании заявок с резолюциями директора ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» и ответственного по защите информации, назначенного приказом директора, готовится проект приказа о допуске сотрудника Учреждения к конфиденциальной информации. Выписка из приказа о допуске к конфиденциальной информации хранится в личном деле сотрудника Учреждения.

3.6. Приказ о допуске сотрудника Учреждения к конфиденциальной информации является основанием допуска его к информационным ресурсам.

3.7. На каждого зарегистрированного пользователя, который имеет доступ в ЛВС, администратор ЛВС заводит учетную карточку (Приложение № 2), в которой отражаются:

- сетевое имя;
- принадлежность к группам;
- имя рабочей станции, с которой разрешен вход в сеть;
- перечень информационных ресурсов, к которым разрешен доступ;
- полномочия по отношению к этим ресурсам и т.д.

Копия карточки передается ответственному по защите информации.

3.8.Ответственный по защите информации, на основании заявок руководителей подразделений Учреждения и учетных карточек пользователей, составляется матрица доступа (таблица разграничения доступа) (Приложение № 3) к защищаемым информационным ресурсам подразделения Учреждения, которая используется им при проведении гласного или негласного контроля.

3.9. Обо всех изменениях в статусе сотрудника Учреждения (увольнение, перемещение по службе, перевод в другое отделение Учреждения), допущенного к конфиденциальной информации, руководитель отделения Учреждения обязан не позднее дня издания приказа уведомлять ответственного по защите информации.

Ответственный по защите информации производит изменения в матрице доступа.

4. ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УЧРЕЖДЕНИЯ

4.1. С целью ограничения доступа к информационным ресурсам АС Учреждения устанавливается система паролирования.

4.1.1. Система паролирования включает в себя следующие основные пароли: системный пароль bios, пользовательский пароль bios, сетевой пароль (личный пароль пользователя), пароль хранителя экрана, личный пароль входа в программу (базу данных).

4.1.2. Личные пароли выбираются пользователями самостоятельно и устанавливаются с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места, слова из словаря и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

4.1.3. Личный пароль является идентификатором (опознавателем) сотрудника, допущенного к информационным ресурсам АС, и составляет его секрет.

4.1.4. Полная плановая смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

4.1.5. Внеплановая смена (удаление) личного пароля любого пользователя АС в случае прекращения его полномочий (увольнение либо

переход на другую работу) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.1.6. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) ответственного по защите информации и других сотрудников Учреждения , которым по роду работы были предоставлены либо полномочия по управлению АС в целом, либо полномочия по управлению подсистемой защиты информации данной АС.

4.1.7. В случае компрометации личного пароля хотя бы одного пользователя АС, необходимо немедленно предпринять меры по смене паролей в объеме, зависимом от полномочий владельца скомпрометированного пароля.

4.1.8. Системные пароли bios, пользовательские пароли bios и пароли хранителя экрана регистрируются в «Книге учета паролей» (Приложение № 4), имеющей гриф – «Для служебного пользования». Доступ к «Книге учета паролей» ограничен. За ее ведение отвечает ответственный по защите информации.

4.1.9. Каждый сотрудник Учреждения, допущенный к информационным ресурсам АС, получает свое пользовательское (сетевое) имя, которое определяется ответственным по защите информации и доводится пользователю.

4.1.10. Сетевое имя и индивидуальный пароль является идентификатором сотрудника Учреждения, допущенного к информационным ресурсам АС, и составляет его секрет.

4.1.11. Пользователь имеет право войти в АС только с тех рабочих станций, которые были указаны руководителем подразделения Учреждения в заявке при регистрации сотрудника Учреждения.

4.1.12. Действия пользователей, допущенных к информационным ресурсам, хранимым на сервере ЛВС, протоколируются. Ответственность за уничтожение и изменение информации несет пользователь, под чьим именем была проведена регистрация.

4.1.13. Все сотрудники Учреждения, допущенные к работе с информационными ресурсами, должны быть ознакомлены под роспись в книге учета паролей с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, за разглашение парольной информации и сохранность информации на отведенных ему разделах сервера.

4.2. Доступ к конфигурации компьютеров и ЛВС.

4.2.1. С целью пресечения несанкционированных действий пользователей, должны выполняться необходимые мероприятия по защите конфигурационных настроек как компьютера, так локальной сети в целом.

4.2.2. С целью обеспечения функционирования «сетевой политики» в программе начальной загрузки должна быть заблокирована возможность загрузки с системной дискеты или компакт-диска (лазерного диска).

4.2.3. Для обеспечения безопасности функционирования ЛВС и данных, устанавливаются ограничения для программ настроек сети, защиты

системы, блокируется возможность настройки сети пользователем, скрываются кнопки организации доступа к файлам и принтерам, делаются недоступными средства редактирования реестра, запрещается запуск программ ms-dos в монопольном режиме, запрещается удаленный доступ к сети и т.д.

4.2.4. Определение политики безопасности функционирования ЛВС возлагается на ответственного по защите информации.

5. ОСОБЕННОСТИ ДОПУСКА В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

5.1. Почтовый ящик служит для приема и отправки документов средствами электронной почты. К данному ресурсу могут иметь полный доступ сотрудники Учреждения, ответственные за прием и отправку электронной почты в Учреждении.

5.2. Допуск к информации, хранимой на дисках отделов.

Данный ресурс представляет собой область для обработки, хранения и обмена информацией внутри Учреждения. Права доступа сотрудника Учреждения к ресурсу (чтение, изменение, удаление, добавление) определяются ответственным по защите информации.

Заместитель директора по безопасности
и АХЧ Н.Б.Фетисова

Приложение № 1
к Положению о разрешительной
системе допуска исполнителей
к конфиденциальной информации

Заявка
на допуск к информационным ресурсам автоматизированных систем Учреждения

Прошу допустить сотрудника (отдела) _____
_____
Наименование управления (отдела), ФИО служащего

к нижепоименованным информационным ресурсам Учреждения:

1. _____
(наименование программы, файла, массива, архива, базы данных и т.п.

с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

2. _____
_____
(наименование программы, файла, массива, архива, базы данных и т.п.

с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

3. _____
(наименование программы, файла, массива, архива, базы данных и т.п.

с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

4. _____
(наименование программы, файла, массива, архива, базы данных и т.п.

с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

5. К информации, содержащейся в почтовом ящике Учреждения (отдела) (Postbox) с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

6. К информации, хранимой на дисках управления (отдела)
с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

7. К информации, содержащейся на диске межсетевого обмена
с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

8. К своему компьютеру с рабочего места _____
наименование рабочего места

Заместитель директора по безопасности и АХЧ _____

Приложение № 2
к Положению о разрешительной
системе допуска исполнителей
к конфиденциальной информации

Лист
персонального учета пользователя ЛВС
№ _____

Фамилия		Дата включения	
Имя		LOGIN	
Отчество		Группа	

Управление (отдел) _____

Занимаемая должность	Дата назначения	Дата отстранения

ВХОЖДЕНИЕ В СЕТЕВЫЕ РАБОЧИЕ ГРУППЫ

№	Наименование рабочей группы	Дата включения	Подпись		Дата отключения	Подпись	
			АБИ	АС		АБИ	АС

ДОПУСК К ЗАЩИЩАЕМЫМ СЕТЕВЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ

№	Информационный ресурс	Уровень доступа	Дата включения	Подпись		Дата отключения	Подпись	
				АБИ	АС		АБИ	АС

ПЕРИОДЫ БЛОКИРОВКИ ДОСТУПА К СЕТИ

№	Причина блокировки	Дата блокировки	Подпись		Дата отмены блокировки	Подпись	
			АБИ	АС		АБИ	АС

РАЗРЕШЕННЫЕ РАБОЧИЕ СТАНЦИИ ДЛЯ ВХОДА В СЕТЬ

№	Сетевое имя компьютера	Дата включения	Подпись		Дата отключения	Подпись	
			АБИ	АС		АБИ	АС

ДОСТУП К СЕТЕВЫМ ПРИНТЕРАМ

№	Сетевое имя принтера	Дата включения	Подпись		Дата отключения	Подпись	
			АБИ	АС		АБИ	АС

ДОСТУП К СУБД

№	Программа	Уровень доступа	Дата включения	Подпись		Дата отключения	Подпись	
				АБИ	АС		АБИ	АС

Ответственный по защите
информации _____

Приложение № 3
к Положению о разрешительной
системе допуска исполнителей
к конфиденциальной информации

Матрица
доступа к разделяемым ресурсам в ЛВС
(Пример заполнения)

№ п\п	Фамилия пользователя	Имя компьютера	Разделяемые ресурсы сервера			
			PUBLIC	BAZA	DELO	TABL
1	Сергеев Д.С.	RSO	RWXD	RWXD	-	-
2	Сидоров С.С.	SSDS	RWXD	-	RWXD	-
3	Краснов Н.А.	Sadmin	RWXD	-	-	RWXD

Примечание: Разграничение прав доступа выполнено средствами ОС _____

Условные обозначения: R - чтение;
W - запись;
X - выполнение программ;
D - удаление.

Матрица
доступа к разделяемым ресурсам рабочей станции RSO
(Пример заполнения)

№ п/п	Фамилия пользователя	Диск С	Разделяемые ресурсы			
			MYDOC	SEC_P	SEC_I	SEC_S
1	Сергеев Д.С.	RWCEDMNGX	RWCEDMNGX	RWCEMGX		
2	Сидоров С.С.	RWCEDMNGX	RWCEDMNGX		RWCEDMNGX	
3	Краснов Н.А.	RWCEDMNGX	RWCEDMNGX			RWCEMGX

Примечание: Разграничение прав доступа выполнено средствами аппаратно-программного комплекса _____

Условные обозначения: R - чтение;
W - запись;
X - выполнение программ;
C - создание файла;
D - удаление файла;
E - переименование файла;
M - создание каталога;
N - удаление каталога;
G - переход в каталог.

Ответственный
по защите информации _____

ПРИЛОЖЕНИЕ №4
к Положению о разрешительной
системе допуска исполнителей
к конфиденциальной информации

ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов»

КНИГА УЧЕТА ПАРОЛЕЙ
пользователей персональных компьютеров

НАЧАТА: _____

ЗАКОНЧЕНА: _____

№ п/п	Ф.И.О. пользователя	Дата установки пароля	Пароль	Роспись пользователя об ознакомлении с главой 4 и п.2.7. Положения о разрешительной системе допуска исполнителей к конфиденциальной информации