УТВЕРЖДЕНО
приказом председателя
Государственного комитета
по делам архивов
Челябинской области

« 08» мая 2015г. № 62

ПОЛОЖЕНИЕ
О РАЗРЕШИТЕЛЬНОЙ СИСТЕМЕ ДОПУСКА ИСПОЛНИТЕЛЕЙ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ КОМИТЕТЕ ПО ДЕЛАМ АРХИВОВ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает единую разрешительную систему допуска к конфиденциальной информации в Государственном комитете по делам архивов Челябинской области (далее – Государственный комитет).

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

1.2. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Сведения, относящиеся к конфиденциальной информации, определяются на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» и Постановлений Правительства Российской Федерации от 03.11.1994 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» и от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», а также ведомственным перечнем сведений, отнесенных к конфиденциальной информации.

1.3. К конфиденциальной информации Государственного комитета также относится конфиденциальная информация (персональные данные) заявителей и работников Государственного комитета.

1.4. К конфиденциальной информации относятся служебные сведения, доступ к которым ограничен в соответствии с действующим законодательством. Порядок обращения с такого рода информацией определяется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 03.11.1994 № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти".

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

2. ДОПУСК К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

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

2.2. Допуск работников Государственного комитета к конфиденциальной информации осуществляется в объеме, необходимом для выполнения должностных обязанностей.

2.3. По своему должностному регламенту председатель Государственного комитета, заместители председателя Государственного комитета, консультант организационно-аналитического отдела Государственного комитета допускаются ко всей конфиденциальной информации Государственного комитета.

2.4. Начальники отделов допускаются к конфиденциальной информации в объеме, необходимом для выполнения стоящих перед отделом задач.

2.5. Работники отделов допускаются к конфиденциальной информации в объеме, необходимом для выполнения своих должностных обязанностей.

2.6. Все работники Государственного комитета должны быть ознакомлены с постановлением Правительства Российской Федерации от 03.11.1994 № 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти" и приказом Росреестра от 10.10.2011 № П/0375/11 «Об организации работы со служебной информацией ограниченного распространения в центральном аппарате Федеральной службы государственной регистрации, кадастра и картографии, ее территориальных органах», а также с обязанностями по ее сохранности и ответственностью в случае ее разглашения (статья 68 Федерального закона от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»).

2.7. Предоставление конфиденциальной информации сторонним организациям регламентируется настоящим Положением.

2.7.1. Предоставление конфиденциальной информации сторонним организациям осуществляется в соответствии:

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

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

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

2.7.3. Основанием для допуска (предоставления информации) является решение председателя Государственного комитета, которое оформляется в виде резолюции.

2.7.4. Предоставление (передача) конфиденциальной информации осуществляется на бумажных, машинных носителях информации и в электронном виде по системе межведомственного взаимодействия.

2.7.5. При наличии официального соглашения со сторонней организацией об обмене информацией, допуск ее осуществляется способом, указанным в подписанном соглашении.

3. ПОРЯДОК ОФОРМЛЕНИЯ ДОПУСКА РАБОТНИКОВ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

3.1. В соответствии с должностными обязанностями работников Государственного комитета необходимость допуска работника к конкретной группе конфиденциальной информации отражается в заявке начальника отдела на имя заместителя председателя Государственного комитета – начальника отдела внедрения автоматизированных архивных технологий.

3.2. Допуск работника к конфиденциальной информации непосредственно не относящейся к выполнению его служебных обязанностей

должен быть обоснован начальником отдела в заявке на имя председателя Государственного комитета, в которой указывается цель ознакомления и время, в течение которого работник допускается к информации.

3.3. Заявка с резолюцией председателя Государственного комитета является основанием для регистрации пользователя в сети и допуска его к конфиденциальным информационным ресурсам.

Заявки хранятся в отделе автоматизированных архивных технологий.

4. ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

4.1. С целью ограничения доступа к информационным ресурсам автоматизированной системы (АС) Государственного комитета устанавливается единая система паролирования.

4.1.1. Система паролирования включает в себя следующие основные пароли: системный пароль (пароль локального администратора), сетевой пароль (личный пароль работника), личный пароль входа в программу (базу данных).

4.1.2. Пароль локального администратора устанавливается специалистом Министерства информационных технологий и связи Челябинской области обслуживающим Государственный комитет.

4.1.3. Личные пароли выбираются работниками самостоятельно, с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, слова из словаря и т.д.), а также общепринятые сокращения (ПЭВМ, ЛВС, user, sysop и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего.

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

4.1.5. Полная плановая смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев.

4.1.6. Внеплановая смена (удаление) личного пароля любого работника (пользователя АС) в случае прекращения его полномочий (увольнение либо переход на другую работу) должна производиться в течение одного рабочего дня после поступления приказа в отдел внедрения автоматизированных архивных технологий.

4.1.7. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) специалистом Министерства информационных технологий и связи Челябинской области, обслуживающим Государственный комитет, работника Государственного комитета, на которого возложены обязанности по защите информации, а также других работников, которым по роду работы были

предоставлены либо полномочия по управлению АС в целом, либо полномочия по управлению подсистемой защиты информации данной АС.

4.1.8. В случае компрометации личного пароля хотя бы одного пользователя АС необходимо немедленно предпринять меры по смене скомпрометированного пароля.

4.1.9. Каждый работник Государственного комитета, допущенный к информационным ресурсам АС, получает свое пользовательское (сетевое) имя, которое составляется системным администратором и доводится пользователю.

4.1.10. Сетевое имя и индивидуальный пароль является идентификатором (опознавателем) работника, допущенного к информационным ресурсам АС, и составляет его секрет.

4.1.11. При входе в АС работник обязан зарегистрироваться под своим пользовательским именем и набрать индивидуальный пароль, после чего он получает доступ к отведенным для него ресурсам.

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

4.1.13. Все работники Государственного комитета, допущенные к работе с информационными ресурсами, должны быть ознакомлены под роспись 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 локальной вычислительной сети (ЛВС).

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

4.2.2. С целью обеспечения функционирования «сетевой политики» в программе начальной загрузки setup должна быть заблокирована возможность загрузки с внешних машинных носителей информации.

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 и т.д.

4.2.4. Реализация и усиление тех или иных ограничений по изменению конфигурационных настроек возлагаются на системного администратора сети, который имеет право изменения групповых политик для осуществления политики информационной безопасности в ЛВС.

5. ОСОБЕННОСТИ ДОПУСКА В ПРОЦЕССЕ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

5.1. Процедура допуска работников Государственного отдела к конфиденциальным информационным ресурсам в автоматизированных информационных системах определяется приказом председателя Государственного комитета.