МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ МОСКОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ
от 1 декабря 2015 г. N 10-33/РВ

ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ ПАРОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ЦЕНТРАЛЬНЫХ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ МОСКОВСКОЙ ОБЛАСТИ И ГОСУДАРСТВЕННЫХ ОРГАНОВ МОСКОВСКОЙ ОБЛАСТИ

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", на основании Положения о Министерстве государственного управления, информационных технологий и связи Московской области, утвержденного постановлением Правительства Московской области от 13 июня 2012 г. N 820/19, в целях совершенствования системы защиты информации центральных исполнительных органов государственной власти Московской области и государственных органов Московской области:

1. Утвердить прилагаемую политику парольной защиты информационных систем центральных исполнительных органов государственной власти Московской области и государственных органов Московской области.

2. Рекомендовать руководителям органов местного самоуправления муниципальных образований Московской области обеспечить исполнение данной политики.

3. Техническую реализацию исполнения данной политики возложить на Государственное казенное учреждение Московской области "Московский областной центр информационно-коммуникационных технологий".

4. Контроль за исполнением настоящего распоряжения возложить на заместителя министра государственного управления, информационных технологий и связи Московской области А.А. Герасимова.

Министр государственного управления,
информационных технологий
и связи Московской области
М.И. Шадаев

Утверждена
распоряжением Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 декабря 2015 г. N 10-33/РВ

ПОЛИТИКА
ПАРОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ЦЕНТРАЛЬНЫХ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ МОСКОВСКОЙ ОБЛАСТИ И ГОСУДАРСТВЕННЫХ ОРГАНОВ МОСКОВСКОЙ ОБЛАСТИ

Перечень используемых сокращений:

АРМ - автоматизированное рабочее место;

АС - автоматизированная система;

ИС - информационная система;

ИСПДн - информационная система персональных данных;

НСД - несанкционированный доступ;

ЦИОГВ и ГО - центральный исполнительный орган государственной власти Московской области и государственный орган Московской области;

ПДн - персональные данные;

ПЭВМ - персональная электронная вычислительная машина;

СрЗИ - средство защиты информации;

ФСБ России - Федеральная служба безопасности Российской Федерации;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю.

1. Общие положения

1.1. Настоящая политика парольной защиты информационных систем центральных исполнительных органов государственной власти Московской области и государственных органов (далее - Политика) определяет порядок парольной защиты ИС ЦИОГВ и ГО и ПЭВМ работников ЦИОГВ и ГО.

1.2. Положения Политики должны учитываться при определении правил генерирования, использования, хранения, смены, прекращения действия паролей доступа к ИС ЦИОГВ и ГО и ПЭВМ работников ЦИОГВ и ГО (далее - пароли).

1.3. Политикой не охватываются вопросы парольной защиты ИС и ПЭВМ, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

1.4. В Политике учтены требования следующих нормативных правовых актов и методических документов в области защиты информации:

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных";

постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

приказ ФСБ России и ФСТЭК России "Об утверждении требований к защите информации, содержащейся в информационных системах общего пользования" от 31 августа 2010 г. N 416/489;

приказ ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

приказ ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения";

Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.;

Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 2 марта 2002 г. N 282.

1.5. В целях исполнения Политики в каждом ЦИОГВ и ГО должны быть разработаны с учетом положений Политики и утверждены руководителем ЦИОГВ и ГО инструкции по обеспечению парольной защиты в ЦИОГВ и ГО.

1.6. Требования к парольной защите каждой отдельной ИС, входящей в состав информационно-технологической инфраструктуры ЦИОГВ и ГО Московской области, должны определяться с учетом положений настоящей Политики.

1.7. Требования к парольной защите каждой отдельной ИС ЦИОГВ и ГО, созданной в целях реализации полномочий ЦИОГВ и ГО, должны учитывать особенности технологического процесса обработки информации в системе, тип системы, а также максимальный уровень конфиденциальности обрабатываемой в ней информации. Требования к парольной защите таких систем должны оформляться документально в виде инструкции по обеспечению парольной защиты в ИС ЦИОГВ и ГО и утверждаться руководителем ЦИОГВ и ГО, эксплуатирующего ИС.

2. Структура централизованного управления паролями

2.1. В целях централизации управления паролями учетные записи пользователей ИС ЦИОГВ и ГО и ПЭВМ работников ЦИОГВ и ГО интегрируются в домен Правительства Московской области - dp.mosreg.ru.

2.2. Структура управления домена Правительства Московской области - dp.mosreg.ru состоит из четырех уровней административной иерархии:

глобальная группа безопасности домена (Enterprise admins) - первый уровень административной иерархии домена, дает права на управление серверами, глобальными параметрами, дочерними доменами, учетными записями. Первоначальная учетная запись администратора создается при установке домена, после чего учетная запись блокируется. Дополнительные временные учетные записи из числа учетных записей группы безопасности администраторов домена (Domain admins) могут быть добавлены в группу безопасности домена (Enterprise admins) только в случае необходимости внесения изменений в схему описания классов объектов единого каталога пользователей (схема LDAP) при установке или обновлении приложений, интегрируемых в схему домена;

администраторы домена (Domain admins) - второй уровень административной иерархии домена, дает права на управление серверами, дочерними доменами, учетными записями, за исключением внесения изменений в схему описания классов объектов единого каталога пользователей (схема LDAP). Учетные записи Domain admins создаются по решению Мингосуправления Московской области и являются постоянными;

группа безопасности домена (<ЦИОГВ и ГО>_admins) - третий уровень административной иерархии домена, на который делегированы права управления учетными записями всех пользователей в разделе домена dp.mosreg.ru соответствующего ЦИОГВ и ГО. Предоставляет права на создание, удаление, изменение учетных записей и объектов групповой политики в разделе домена dp.mosreg.ru соответствующего ЦИОГВ и ГО;

персонализированная учетная запись локального администратора (<ЦИОГВ и ГО>_local_admin) - четвертый уровень административной иерархии домена, на который делегированы права локального администрирования всех ПЭВМ и серверов, зарегистрированных в разделе домена dp.mosreg.ru соответствующего ЦИОГВ и ГО, учетная запись создается путем применения групповой политики.

2.3. Интеграция учетных записей ИС ЦИОГВ и ГО и ПЭВМ работников ЦИОГВ и ГО в домен Правительства Московской области dp.mosreg.ru обеспечивается Мингосуправления Московской области при содействии ЦИОГВ и ГО.

3. Порядок генерирования, использования, хранения, смены, прекращения действия паролей доступа в ИС ЦИОГВ и ГО

3.1. Организационное и техническое обеспечение управления паролями возлагается на отдел (управление, ответственных лиц) по защите информации ЦИОГВ и ГО или его структурное подразделение, эксплуатирующее ИС либо ПЭВМ; организация и проведение мероприятий по генерированию, использованию, хранению, смене, прекращению действия паролей - на администраторов соответствующего уровня административной иерархии домена dp.mosreg.ru, контроль за исполнением Политики в ЦИОГВ и ГО - на руководителей ЦИОГВ и ГО.

3.2. Правила управления паролями.

Управление личными паролями пользователей производится централизованно с помощью применения средств единой службы каталогов Active Directory. Обеспечение централизованного управления указанными средствами возлагается на Мингосуправления Московской области. Управление групповыми политиками осуществляется отделом (управлением, ответственными лицами) по защите информации ЦИОГВ и ГО или его структурным подразделением, эксплуатирующим ИС либо ПЭВМ. Генерация персональных паролей пользователей осуществляется пользователями с учетом ограничений, предусмотренных соответствующими групповыми политиками.

3.3. Требования к паролям.

Минимальная длина пароля пользователя ИС определяется уровнем важности информации, обрабатываемой в ИС. При этом длина пароля должна быть не менее восьми символов.

Пароль должен включать в себя символы как минимум трех различных типов (например, цифры и буквы верхнего и нижнего регистра).

Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования ИС и другие), а также общепринятые сокращения и любые другие данные, которые можно определить исходя из информации о пользователе (даты рождения родственников, клички домашних животных и подобные).

Пароль не должен включать в себя последовательности из более чем 2 символов, расположенных рядом на клавиатуре (например, 123, qwe и другие).

Пароль не должен состоять из одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов (например, 222999, psqpsq).

Запрещается использование паролей, заданных по умолчанию производителями применяемых программных и аппаратных средств обработки и защиты информации.

Требования, указанные в данном пункте Политики, должны быть учтены при формировании объектов групповой политики. Ответственность за формирование указанных объектов возлагается на администраторов соответствующего уровня административной иерархии домена dp.mosreg.ru.

Для генерации паролей могут применяться специальные программные средства, как автономные, так и входящие в состав установленных на ПЭВМ СрЗИ. При этом пароли, сгенерированные такими средствами, должны удовлетворять всем требованиям, указанным в данном пункте Политики.

3.4. Правила использования паролей.

При использовании паролей пользователь обязан соблюдать положения должностных инструкций, методических документов по защите информации, а также данной Политики.

Ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан.

При вводе паролей необходимо исключить возможность его просмотра посторонними лицами или техническими средствами (фото-, видеокамеры и другие средства).

Пользователь не имеет права сообщать личный пароль другим пользователям и допускать их к работе в своей учетной записи в ИС.

При утере, компрометации, несанкционированном изменении паролей пользователь обязан своевременно сообщать администратору безопасности (при его наличии) ИС либо лицу, ответственному за защиту информации в соответствующем ЦИОГВ и ГО (его структурном подразделении).

3.5. Правила хранения паролей.

При хранении паролей должны быть приняты все возможные меры по минимизации возможности компрометации либо утери пароля.

Запрещается:

записывать пароли в файлах, электронных записных книжках, других электронных носителях информации;

указывать пароли на бумажных и других материальных носителях информации, в том числе на предметах, -

за исключением случаев, предусмотренных Политикой.

Запрещается хранение паролей в ИС в открытом виде.

Хранение пользователем паролей на материальном либо электронном носителе допускается только в личном сейфе владельца пароля либо в сейфе у руководителя подразделения. При этом должны быть приняты меры, препятствующие компрометации пароля другими лицами (например, хранение в пенале, опечатанном личной печатью пользователя).

3.6. Правила смены паролей.

Плановая смена паролей пользователя должна проводиться регулярно и не реже указанных в данном пункте сроков.

В ИС, аттестованных по требованиям безопасности информации, плановая смена паролей пользователей должна проводиться в соответствии с требованиями, указанными в аттестационной и организационно-распорядительной документации на ИС, но не реже 1 раза в 90 дней.

В прочих ИС, в том числе предназначенных для обработки ПДн и государственных информационных ресурсов, плановая смена паролей пользователей должна проводиться не реже 1 раза в 90 дней.

В случае компрометации либо утери пароля незамедлительно должна проводиться его внеплановая смена. При этом пользователь обязан обратиться к администратору безопасности ИС (при его наличии) либо лицу, ответственному за защиту информации в соответствующем ЦИОГВ и ГО (его структурном подразделении).

Внеплановая смена паролей может проводиться по распоряжению ответственного за защиту информации в ЦИОГВ и ГО (его структурном подразделении) после обнаружения фактов попыток НСД, компрометации пароля либо других нештатных ситуаций.

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 символах.

При смене пароля новое значение не должно совпадать с 10 предыдущими значениями паролей доступа данного пользователя.

3.7. Правила прекращения действия паролей.

Прекращение действия пароля возможно при истечении срока его действия, внеплановой смене, утере либо удалении учетной записи.

В случае прекращения полномочий пользователя, в том числе увольнения, перехода на другую работу, в обязательном порядке производится удаление его учетной записи и пароля немедленно после окончания последнего сеанса работы данного пользователя с системой. При окончании или прекращении полномочий пользователей не допускается сохранение или передача другим пользователям их учетных записей и паролей.

Запрещается разглашение паролей после прекращения их действия.

4. Реализация Политики в ЦИОГВ и ГО

4.1. Реализация Политики в ЦИОГВ и ГО осуществляется за счет согласованных действий руководителя ЦИОГВ и ГО, лиц, ответственных за защиту информации в ЦИОГВ и ГО, администраторов соответствующего уровня административной иерархии домена dp.mosreg.ru в ЦИОГВ и ГО, администраторов безопасности ИС (при их наличии), а также пользователей ИС ЦИОГВ и ГО и ПЭВМ работников ЦИОГВ и ГО.

4.2. Руководитель ЦИОГВ и ГО:

назначает ответственного (ответственных) за обеспечение защиты информации в ЦИОГВ и ГО соответствующим приказом;

при необходимости назначает администраторов безопасности ИС ЦИОГВ и ГО соответствующими приказами;

утверждает инструкцию по обеспечению парольной защиты в ЦИОГВ и ГО и при необходимости инструкции по обеспечению парольной защиты в ИС ЦИОГВ и ГО;

осуществляет контроль за исполнением Политики в ЦИОГВ и ГО;

организовывает расследование инцидентов, связанных с нарушениями Политики в ЦИОГВ и ГО;

устанавливает ответственность работников ЦИОГВ и ГО за нарушение Политики;

при осуществлении своих полномочий соблюдает требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению парольной защиты в ЦИОГВ и ГО, а также инструкций по обеспечению парольной защиты в ИС (при их наличии).

4.3. Ответственный за обеспечение защиты информации в ЦИОГВ и ГО:

осуществляет контроль за действиями администраторов соответствующего уровня административной иерархии домена dp.mosreg.ru в ЦИОГВ и ГО;

формирует требования к объектам групповой политики в ЦИОГВ и ГО с учетом положений Политики;

организовывает проведение периодического контроля соблюдения требований информационной безопасности в ЦИОГВ и ГО при работе с паролями;

проводит сбор и анализ информации об учетных записях работников ЦИОГВ и ГО, а также предоставление указанной информации в Мингосуправления Московской области;

проводит сбор и анализ информации об инцидентах информационной безопасности, связанных с нарушениями Политики в ЦИОГВ и ГО, а также предоставление указанной информации в Мингосуправления Московской области;

проводит расследование инцидентов, связанных с нарушениями Политики в ЦИОГВ и ГО;

при осуществлении своих полномочий соблюдает требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению парольной защиты в ЦИОГВ и ГО, а также инструкций по обеспечению парольной защиты в ИС (при их наличии).

4.4. Администраторы соответствующего уровня административной иерархии домена dp.mosreg.ru в ЦИОГВ и ГО:

осуществляют создание и редактирование групповых политик для управления учетными записями работников ЦИОГВ и ГО;

осуществляют создание учетных записей работников ЦИОГВ и ГО и генерацию первичных паролей;

при необходимости осуществляют принудительную смену паролей и удаление учетных записей;

осуществляют регистрацию и учет информации об учетных записях работников ЦИОГВ и ГО и об инцидентах, связанных с нарушениями Политики в ЦИОГВ и ГО, а также предоставляют указанную информацию ответственным за обеспечение защиты информации в ЦИОГВ и ГО;

участвуют в расследовании инцидентов, связанных с нарушениями Политики в ЦИОГВ и ГО;

проводят повседневный контроль действий работников ЦИОГВ и ГО при работе с паролями;

проводят разъяснительную и консультационную работу с работниками ЦИОГВ и ГО в части управления и пользования паролями;

при осуществлении своих полномочий соблюдают требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению парольной защиты в ЦИОГВ и ГО, а также инструкций по обеспечению парольной защиты в ИС (при их наличии).

4.5. Администраторы безопасности ИС:

осуществляют установку и настройку средств защиты информации ИС в соответствии с требованиями законодательства Российской Федерации и Московской области в области защиты информации;

осуществляют создание учетных записей пользователей ИС и генерацию первичных паролей;

при необходимости осуществляют принудительную смену паролей и удаление учетных записей пользователей ИС;

участвуют в расследовании инцидентов информационной безопасности, связанных с нарушениями Политики в ИС;

проводят повседневный контроль действий пользователей ИС при работе с паролями;

проводят разъяснительную и консультационную работу с пользователями ИС в части управления и пользования паролями;

при осуществлении своих полномочий соблюдают требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению парольной защиты в ЦИОГВ и ГО, а также инструкций по обеспечению парольной защиты в ИС.

4.6. Работники ЦИОГВ и ГО:

при необходимости получения учетной записи направляют соответствующую заявку администратору соответствующего уровня административной иерархии домена dp.mosreg.ru в ЦИОГВ и ГО;

при первом сеансе работы со своей учетной записью немедленно производят смену первичного пароля, предоставленного администратором соответствующего уровня административной иерархии домена dp.mosreg.ru в ЦИОГВ и ГО, с учетом требований групповой политики;

при получении сообщения об истечении срока действия личного пароля производят генерацию пароля и его смену с учетом требований групповой политики;

при компрометации либо утере личного пароля немедленно уведомляют администратора безопасности (при его наличии) и ответственного за обеспечение защиты информации в ЦИОГВ и ГО и следуют соответствующим инструкциям;

при пользовании личным паролем соблюдают требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению парольной защиты в ЦИОГВ и ГО, а также инструкций по обеспечению парольной защиты в ИС (при их наличии).

5. Контроль соблюдения Политики и ответственность

за ее нарушение

5.1. Контроль за соблюдением порядка управления паролями с помощью применения средств единой службы каталогов Active Directory возлагается на Мингосуправления Московской области.

5.2. Контроль за исполнением Политики в ЦИОГВ и ГО возлагается на руководителей ЦИОГВ и ГО.

5.3. В целях обеспечения контроля за соблюдением порядка управления паролями ЦИОГВ и ГО:

предоставляют Мингосуправления Московской области ежеквартально сводки по работникам ЦИОГВ и ГО, для которых требуется наличие учетной записи в единой службе каталогов Active Directory. Мингосуправления Московской области проводит анализ полученных сводок на предмет соответствия существующих учетных записей требуемым;

в трехдневный срок уведомляют Мингосуправления Московской области о прекращении полномочий работников, у которых имеется учетная запись в единой службе каталогов Active Directory. После получения уведомления Мингосуправления Московской области в течение следующего рабочего дня производит проверку факта удаления учетной записи пользователя из единой службы каталогов Active Directory администратором соответствующего уровня административной иерархии домена dp.mosreg.ru (при необходимости удаление учетной записи);

в трехдневный срок уведомляют Мингосуправления Московской области о фактах компрометации паролей и других инцидентах в части управления паролями, а также о действиях, направленных на устранение последствий указанных инцидентов и недопущение их повторения в дальнейшем.

5.4. Повседневный контроль действий пользователей и обслуживающего персонала при работе с паролями, их смене, хранении возлагается на администратора безопасности ИС (при наличии) и администраторов соответствующего уровня административной иерархии домена dp.mosreg.ru.

5.5. Периодический контроль соблюдения информационной безопасности в ЦИОГВ и ГО при работе с паролями, их смене, хранении возлагается на лицо, ответственное за обеспечение защиты информации в ЦИОГВ и ГО (его структурном подразделении).

5.6. Лица, участвующие в процессах управления паролями, описанных в Политике, несут ответственность за выполнение возлагаемых на них функциональных обязанностей в соответствии с законодательством Российской Федерации и Московской области.