УТВЕРЖДЕНА
приказом государственного автономного
учреждения Республики Коми
«Центр информационных технологий»
от 19.08.2020 № 94
(приложение № 2)

ПОЛИТИКА
информационной безопасности
«Парольная политика»

1. Общие положения

Настоящая политика информационной безопасности «Парольная политика» (далее – Политика) определяет обязательные требования к минимальным характеристикам, защите и передаче паролей пользователей ГИТС и администраторов ГИТС.

2. Термины и обозначения

Администратор ГИТС – работник ГАУ РК «ЦИТ» и сторонней организации, осуществляющий администрирование ресурсов ГИТС.

АРМ – автоматизированное рабочее место - компьютер, включенный в ЛВС и предоставляющий пользователю доступ к ее ресурсам.

ГАУ РК «ЦИТ» - государственное автономное учреждение Республики Коми «Центр информационных технологий». На основании постановления Правительства Республики Коми от 21 марта 2011 г. № 60 ГАУ РК «ЦИТ» является оператором ГИТС, осуществляющим техническое, организационное управление и эксплуатацию ГИТС.

ГИС – государственная информационная система Республики Коми.

ГИТС - государственная информационно-телекоммуникационная сеть Республики Коми. Компоненты ГИТС: ЦТУ, базовая ЛВС - ЛВС в зданиях, находящихся по адресам: г. Сыктывкар, ул. Коммунистическая, д. 9 и ул. Коммунистическая, д. 8, выделенные каналы передачи данных, объединяющие ЛВС в других зданиях, в которых расположены пользователи ГИТС.

ЗОКИИ - значимые объекты критической информационной инфраструктуры органов государственной власти Республики Коми и государственных учреждений Республики Коми.

ИС - информационная система.

ЛВС - локальная вычислительная сеть - программно-аппаратный комплекс, включающий в себя компьютеры, периферийное оборудование с сетевыми интерфейсами, коммуникационное оборудование, кабельную систему и сетевые операционные системы, предназначенный для совместного использования информационных ресурсов в пределах организации либо в

пределах ограниченной территории (в том числе здания, комплекса зданий, технической площадки).

ОС – операционная система.

Пользователь ГИТС - субъект, правомочно осуществляющий доступ к ресурсам ГИТС.

Ресурсы ГИТС - вычислительная мощность оборудования и иных средств, составляющих ГИТС (серверов, их дискового пространства, сетевого периферийного оборудования, сетевых сервисов, массивов информации, программных средств, предоставленных пользователям ГИТС).

СЗИ - средство защиты информации.

ЦТУ - центральный телекоммуникационный узел - основное звено ГИТС, интегрирующее ресурсы ГИТС, располагается в помещениях центра обработки данных ГАУ РК «ЦИТ».

3. Требования к характеристикам паролей

3.1. Пароли, используемые для аутентификации в ОС, ГИС, ЗОКИИ, иных ИС и СЗИ, а также пароли, используемые для доступа к настройкам сетевого, коммутационного оборудования, должны отвечать минимальным характеристикам паролей и не подпадать под характеристики слабых паролей, указанных в приложении к настоящей Политике.

3.2. Пароли пользователей ГИТС, используемые для аутентификации в ГИС и ЗОКИИ, должны отвечать тем же минимальным характеристикам, что и пароли администраторов ГИТС, если иное не установлено в аттестационных документах на соответствующую ГИС или ЗОКИИ.

3.3. Алфавит пароля должен быть не менее 70 символов.

3.4. В ОС, ГИС, ЗОКИИ, иных ИС максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток. В случае достижения установленного максимального количества неуспешных попыток аутентификации должна быть осуществлена блокировка программно-технического средства или учетной записи пользователя от 15 до 60 минут.

4. Требования и рекомендации к передаче, генерации, смене и хранению паролей

4.1. Передачу паролей рекомендуется осуществлять посредством Системы генерации и передачи паролей ГАУ РК «ЦИТ» (сайт pwd.rkomi.ru) или по защищенным каналам связи (например, с помощью VPN соединения), или в защищенном виде (например, с помощью зашифрованного архива). При отсутствии возможности передачи пароля вышеуказанными способами в исключительных случаях пароль может быть передан по телефону или SMS сообщением.

4.2. После получения пароля Пользователям ГИТС рекомендуется, при наличии возможности, сменить его с использованием генераторов

случайных паролей или на основании парольной фразы в соответствии с требованиями к минимальным характеристикам таких паролей.

4.3. Для генерации паролей рекомендуется использовать Систему генерации и передачи паролей ГАУ РК «ЦИТ» (сайт pwd.rkomi.ru), либо ПО, локально установленное на АРМ или на сервере в ЦТУ ГИТС.

4.4. Для Администраторов ГИТС действие пункта 4.3 настоящей Политики носит обязательный характер.

4.5. Пользователи ГИТС и Администраторы ГИТС обязаны:

– хранить пароли в тайне;

– не сообщать и не передавать пароли третьим лицам (например, друзьям, коллегам, руководителю и т.п.) за исключением случаев, предусмотренных пунктом 4.6 настоящей Политики.

4.6. Передачу паролей разрешается осуществлять в следующих случаях:

4.6.1. Передача пароля от работника руководителю структурного подразделения при возникновении производственной необходимости в случае временного отсутствия работника.

4.6.2. Передача паролей от работника руководителю подразделения в случае прекращения его полномочий (увольнение и т.п.).

4.6.3. Передача паролей между работниками в случае использования общих учетных записей или общих адресов рабочей электронной почты для исполнения должностных обязанностей.

4.6.4. В случае необходимости передача паролей Администраторами ИС в отдел администрирования инфраструктуры электронного правительства Республики Коми ГАУ РК «ЦИТ» для обеспечения работоспособности ИС.

4.6.5. Передача паролей для хранения руководителю структурного подразделения в соответствии с пунктом 4.12 настоящей Политики.

4.7. В случаях, указанных в пунктах 4.6.1 - 4.6.4 настоящей Политики, передача пароля осуществляется в соответствии с пунктом 4.2 настоящей Политики.

4.8. Пользователи ГИТС обязаны самостоятельно производить смену паролей по истечении 90 дней с момента их последнего изменения, при отсутствии возможности самостоятельной смены пароля - обратиться к администратору ГИТС.

4.9. Администраторы ГИТС обязаны самостоятельно производить смену паролей по истечении 60 дней с момента их последнего изменения.

4.10. Смена паролей, используемых для доступа к настройкам сетевого или коммутационного оборудования, а также СЗИ производится по усмотрению ответственного лица, при условии соответствия сложности пароля минимальным характеристикам безопасности.

4.11. В случае прекращения полномочий (увольнение и т.п.) работника, который имел доступ к сервисным, системным или общим учетным записям, должна производиться смена паролей данных учетных записей.

4.12. Хранение паролей на бумажном носителе допускается только в личном сейфе (или в личном опечатываемом, запирающемся шкафу) или в сейфе (или в опечатываемом, запирающемся шкафу) руководителя подразделения в закрытом конверте. При возникновении производственной необходимости в случае временного отсутствия работника или в случае прекращения его полномочий (увольнение и т.п.) руководителю подразделения разрешается вскрыть конверт с паролем.

4.13. Допустимо хранение паролей Пользователей ГИТС на АРМ в файлах, не доступных другим пользователям (т.е. исключительно на локальных дисках, не на сетевых и не в общих папках). В таких случаях рекомендуется хранить пароли в зашифрованном виде (например, с помощью программы KeePass, зашифрованного архива и т.п.).

4.14. Хранение паролей Администраторов ГИТС может осуществляться только в зашифрованном виде (например, с помощью программы KeePass, зашифрованного архива и т.п.).

4.15. Информацию о попытках получения или требования пароля третьими лицами работникам необходимо сообщать непосредственному руководителю.

Приложение
к Политике информационной
безопасности
«Парольная политика»

ТРЕБОВАНИЯ
к минимальным характеристикам паролей

Минимальные характеристики паролей Пользователей ГИТС:

– не менее 8 символов;

– состоит из комбинации не менее 3-х групп символов из предложенных: строчные буквы, прописные буквы, цифры, специальные символы.

Минимальные характеристики паролей Администраторов ГИТС:

– не менее 8 символов;

– состоит из комбинации 4-х групп символов из предложенных: строчные буквы, прописные буквы, цифры, специальные символы.

Минимальные характеристики паролей, используемых для доступа к настройкам сетевого, коммутационного оборудования, и паролей, используемых в СЗИ:

– не менее 12 символов;

– состав пароля: латинские буквы, специальные символы и (или) цифры;

– пароль формируется при помощи специальных программ, предназначенных для генерации парольных фраз.

Характеристики слабых паролей:

– состоящие из повторяющегося символа или группы символов (*например, 1111qqqq, 123123123*);

– состоящие из символов, расположенных на клавиатуре подряд (*например, qwerty123*);

– содержащие стандартные фразы (*например, St@ndart1, Pa$$word и др.*);

– используемые для авторизации в социальных сетях, почтовых сервисах, на форумах или на домашних персональных компьютерах.