ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
Комитет по образованию
Администрация Центрального района
Государственное бюджетное учреждение
дополнительного образования
Центр внешкольной работы Центрального района Санкт-Петербурга

П Р И К А З

№ 180/2 31 мая 2016 г.

Об утверждении
Положения о парольной защите

В целях защиты персональных данных, используемых в ГБУ ДО ЦВР Центрального района СПб, а также в целях повышения эффективности ограничения доступа обучающихся, педагогических работников и иных сотрудников образовательного учреждения к ресурсам, не совместимым с задачами образования и воспитания и их сопровождения, и на основании решения Педагогического совета (Протокол № 2 от 31.05.2016),

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положения о парольной защите;
2. Контроль за исполнением приказа оставляю за собой.

Приложение:

1. Положение о парольной защите в ГБУ ДО ЦВР Центрального района СПб

Директор В.А. Педан

Приложение № 1 к приказу
№ 180/2 от 31.05.2016

ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
Комитет по образованию
Администрация Центрального района
Государственное бюджетное учреждение
дополнительного образования
Центр внешкольной работы Центрального района Санкт-Петербурга

Принято
решением Педагогического совета
Протокол № 2 от 31.05.2016

Утверждаю
директор ГБУ ДО ЦВР Центрального района СПб
_____ В.А. Педан
31 мая 2016 г.

Положение о парольной защите в ГБУ ДО ЦВР Центрального района СПб

Раздел I. Общие положения

1.1. Введение

Для обеспечения конфиденциальности, целостности, ограничения несанкционированного доступа в информационные системы в ГБУ ДО ЦВР Центрального района СПб (далее – учреждение) используется, наряду с другими средствами, парольная защита. Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

1.2. Цель

Положение определяет требования учреждения к парольной защите информационных систем.

1.3. Область действия

Положение распространяется на всех пользователей и информационные системы (далее – ИС) учреждения, использующих парольную защиту.

Раздел II. Термины и определения

Аутентификация – установление того, что пользователь является именно тем, кем он себя объявил путем проверки предъявленного пароля.

Инициализационный пароль – пароль, выдаваемый пользователю для первоначального входа в ИС.

ИС – в данном случае любая информационная система, для работы с которой необходима аутентификация пользователя (рабочие станции – ПК, электронная почта, системы бухгалтерского учета и т.п.).

Компрометация пароля – известность пароля или принципа его формирования посторонним лицам.

Ответственный за работу ИС учреждения – сотрудник учреждения, который в силу должностных обязанностей, занимается обслуживанием информационных систем, телекоммуникационного оборудования и т.п. (инженер-системный администратор).

Пароль – секретный набор символов, используемый для аутентификации пользователя.

Пользователи – администраторы ИС и иные сотрудники учреждения или сторонней организации, которым предоставлен доступ к ИС учреждения, а также корпоративный доступ к ресурсам сети Интернет.

Учетная запись – идентификатор пользователя, используемый для доступа к ИС.

Раздел III. Положения

3.1. Каждая учетная запись в информационных системах должна быть защищена паролем.

3.2. В зависимости от настроек ИС, пользователю выдается либо постоянный пароль, либо инициализационный пароль, который он обязан сменить при первом входе в ИС.

3.3. Пользователь обязан использовать различные пароли для каждой учетной записи.

3.4. Учетная запись пользователя блокируется после нескольких неудачных попыток ввода пароля. Разблокировка учетной записи возможна только через специальную процедуру восстановления пароля, определяемой настройками информационной системы.

3.5. Пользователь обязан менять пароли для доступа к корпоративным ИС не реже чем раз в 180 календарных дней.

3.6. При выборе пароля пользователь обязан соблюдать следующие требования:

— Минимальная длина пароля пользователя составляет не менее 8-ми символов;

— Пароль должен состоять из комбинации цифр, букв латинского алфавита верхнего и нижнего регистра;

— Новый пароль не должен повторять использованные ранее пароли.

3.7. Пользователь обязан применять адекватные меры по защите своих паролей:

— Запоминать свои пароли или хранить их таким образом, чтобы они были недоступны третьим лицам;

— Не передавать свои пароли никому ни под каким предлогом, включая коллег, обучающихся, родственников или знакомых;

— При использовании пароля (например, его вводе) принять необходимые меры, исключающие возможность его компрометации (например, исключить возможность подглядывания вводимого пароля).

3.8. Пользователю запрещено создавать условия для несанкционированного доступа к информационным системам и материалам, которые не предназначены для третьих лиц (включая обучающихся и других сотрудников). Таковыми условиями могут быть, например, оставление ПК незаблокированным при покидании рабочего места; вход в веб-интерфейс корпоративной электронной почты на ПК, не предназначенных для конкретного сотрудника (на ПК другого сотрудника, домашнем ПК), и отсутствие действий по адекватному выходу из учётной записи; вход в иные ИС и неадекватные меры защиты от доступа в них третьих лиц и т.п.

3.9. Пользователю запрещено применять пароли, используемые им при аутентификации в ИС учреждения, для доступа в не принадлежащие учреждению ИС (например, на веб-сайтах сети Интернет и др.).

3.10. В случае компрометации или подозрения на компрометацию пароля, пользователь обязан информировать об этом ответственного за работу ИС учреждения и немедленно сменить пароль.

3.11. Пароли встроенных административных учетных записей (например, «root» в ОС UNIX, «Administrator» в MS Windows и т.п.) основных ИС, а также пароль локального администратора рабочих станций филиала должны храниться в защищенном месте. Доступ к этим паролям возможен только ответственному за работу ИС учреждения и руководителю учреждения.

3.12. Учетные записи сотрудников, имеющих членство в группах администраторов, должны иметь пароль, отличный от всех других паролей данного пользователя.

3.13. Ответственному за работу ИС учреждения запрещено хранить пароли пользователей в открытом виде или в виде хеш-функций, а также размещать пароли на ресурсах общего доступа, или пересылать их по электронной почте, за исключением пересылки пользователю инициализированного пароля.

3.14. При использовании программного обеспечения, аппаратных комплексов и другого оборудования не допускается использование значений пары логин-пароль заданных по умолчанию.

3.15. Смена паролей административных учетных записей, используемых на серверах и маршрутизирующем оборудовании, а также пароля локального администратора рабочих станций филиала, иных пользователей обязательно производится в следующих случаях:

— Компрометация, либо подозрение на компрометацию паролей;

— Увольнение из учреждения лиц, которым в связи с производственной необходимостью были известны пароли;

— Расторжение договора с подрядной организацией, сотрудникам которой выдавались пароли для выполнения работ на оборудовании учреждения.

3.16. При наступлении случаев, описанных в п. 3.14, создается новый пароль, который хранится в месте и в виде, которые исключают компрометацию паролей.

Раздел IV. Роли и ответственность

4.1. Пользователи:

— Исполняют требования положения и несут ответственность за ее нарушение;

— Информируют ответственного за работу ИС учреждения обо всех ставших им известных случаях нарушения настоящего положения.

4.2. Ответственный за работу ИС учреждения:

— Принимает обращения пользователей по вопросам парольной защиты (например, блокировка учетных записей, компрометация пароля, нарушение положения и др.), при необходимости, ведет их учет;

— Консультирует пользователей по вопросам использования парольной защиты;

— Выдает пользователям инициализационные пароли для входа в ИС;

— Отвечает за безопасное хранение паролей встроенных административных учетных записей;

— Производит разблокировку учетных записей пользователей.

4.3. За нарушение требований настоящего Положения на сотрудника учреждения может быть наложено дисциплинарное или административное взыскание.