

ПРИНЯТО
педагогическим советом
30 августа 2016 года
протокол №1



УТВЕРЖДАЮ

и. о. директора Трегубов О. В.
Приказ № 61-А от 31 августа 2016 года

Приложение №2

Положение по организации парольной защиты в МБОУСОШ №5

Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты и регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИСПД - информационная система персональных данных.

Компрометация - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль - уникальный признак субъекта доступа, который является его (субъекта) секретом.

Правила доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Несанкционированный доступ (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированной системы (далее - АС).

Правила генерации паролей

Персональные пароли должны генерироваться специальными программными средствами административной службы.

Длина пароля должна быть не менее 8 символов.

В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

Пароль не должен включать в себя:

легко вычисляемые сочетания символов;

клавиатурные последовательности символов и знаков;

общепринятые сокращения;

аббревиатуры;

номера телефонов, автомобилей;

прочие сочетания букв и знаков, ассоциируемые с пользователем;

при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПД объекта образования.

Порядок смены паролей

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца.

Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной защитой.

Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПД.

В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

Обязанности пользователей при работе с парольной защитой

При работе с парольной защитой пользователям запрещается:

разглашать кому-либо персональный пароль и прочие идентифицирующие сведения; предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПД, посторонним лицам;

записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе.

При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

Случаи компрометации паролей

Под компрометацией следует понимать следующее:

физическая утеря носителя с информацией;

передача идентификационной информации по открытым каналам связи;

проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма, или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);

визуальный осмотр носителя идентификационной информации посторонним лицом;

перехват пароля при распределении идентификаторов;

сознательная передача информации постороннему лицу.

Действия при компрометации пароля:

скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;

о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

Ответственность пользователей при работе с парольной защитой

Повседневный контроль за действиями сотрудников ОУ при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

Владельцы паролей должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

Ответственность в случае несвоевременного уведомления ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.