Муниципальное дошкольное образовательное учреждение
«Осьминский детский сад»
(МДОУ «Осьминский детский сад»)

СОГЛАСОВАНО
Общим собранием родителей
МДОУ «Осьминский детский сад»
(протокол от *20.11.2019* № 02*)*

УТВЕРЖДЕНО
Приказом № 74 от 20.11.2019г.
МДОУ «Осьминский детский сад»

ПОЛОЖЕНИЕ

о парольной защите при обработке персональных данных и иной конфиденциальной информации

1. Общие положения.

Настоящее положение устанавливает основные правила введения парольной защиты

информационной системы персональных данных в Муниципальном дошкольном образовательном учреждении «Осьминский детский сад» (далее - Учреждение). Положение регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями.

Настоящее положение оперирует следующими основными понятиями:

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

ИСПДн - 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 – доступ к информации, нарушающий правила

разграничения доступа с использованием штатных средств, предоставляемых средствами

вычислительной техники или АС.

Организационное и техническое обеспечение процессов генерации, использования,

смены и прекращения действия паролей во всех ИС и контроль за действиями пользователей и обслуживающего персонала при работе с паролями возлагается на сотрудников МДОУ, работающих с автоматизированными информационными системами (АИС *или иного соответствующего подразделения (или уполномоченного лица) Оператора*) – администраторов парольной защиты.

2. Правила генерации паролей

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

2.2. Длина пароля должна быть не менее 8 символов.

2.3. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

2.4. 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 (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

-при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

- личный пароль Пользователь не имеет права сообщать никому.

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

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

2.7. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*). Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) с паролями других сотрудников подразделений Оператора.

3. Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в три месяца.

3.2 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 зашитой.
3.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.
3.4 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.

4. Обязанности пользователей при работе с парольной защитой

4.1. 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 ИСПДн посторонним лицам;
записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах к которым могут иметь свободный доступ иные лица.
4.2. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними липами и техническими средствами.

5. Случаи компрометации паролей

5.1. Под компрометацией следует понимать: 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.
5.2. 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.

6. Ответственность пользователей при работе с парольной защитой

6.1. Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
6.2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
6.3. Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
6.4. Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.