

СОГЛАСОВАНО:
на Заседании Совета
Учреждения
Протокол №11 от 22.11.2021

ПРИНЯТО:
на Педагогическом совете
Протокол №14 от
23.11.2021 г.

УТВЕРЖДЕНО:
Приказом директора № 01-
06/210-осн от 27.12.2021 г.

ПОЛОЖЕНИЕ

об обеспечении безопасности общедоступной информации при ее обработке в информационных системах

1. Общие положения

1.1. Положение об обеспечении безопасности общедоступной информации при ее обработке в информационных системах МБОУ «СОШ №103» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой и защитой информации в целях реализации мер по обеспечению безопасности общедоступной информации при ее обработке в информационных системах МБОУ «СОШ №103» (далее - школа).

1.2. Положение устанавливает требования к обеспечению безопасности общедоступной информации (далее - ОИ) в информационных системах (далее - ИС) школы, доступ к которой не ограничен федеральными законами.

К ОИ относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Любыми лицами по их усмотрению может использоваться ОИ при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Под ИС понимается совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (далее - ТС), расположенных в здании школы по адресу: ул. Дёповская, 32.

ИС используются для хранения, обработки и передачи информации в соответствии с функциями, возложенными на школы.

ИС включают в себя:

- аппаратно-программный комплекс;
- рабочие станции, сетевое оборудование, периферийное оборудование (принтеры, сканеры и т.п.) и другое специализированное оборудование школы.

1.3. Безопасность ОИ при ее обработке в ИС школы обеспечивается применением организационных мер и ТС защиты информации, реализующих требования нормативных правовых актов Российской Федерации.

1.4. Требования Положения и других документов, разработанных для их реализации, являются обязательными для исполнения всеми лицами,

получившими доступ к ОИ в ИС школы, и должны быть доведены до их сведения.

1.5. Решение о необходимости внесения изменений и дополнений в Положение принимается на основании:

- результатов анализа инцидентов информационной безопасности в ИС;
- изменения технологии обработки информации;
- изменения нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой и защитой информации.

2. Цель защиты информации и основные виды угроз безопасности

2.1. Основной целью защиты информации является обеспечение принятия организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, от иных неправомерных действий в отношении такой информации;

- реализацию прав на доступ к информации.

2.2. На основании Положения устанавливаются требования:

- разграничения доступа к ОИ, порядка и условий такого доступа;
- обработки информации;
- передачи информации другим лицам по договору или на ином установленном законном основании.

2.3. Основными видами угроз безопасности ОИ в ИС являются:

- противоправные и (или) ошибочные действия пользователей ИС и третьих лиц;

- отказы, сбои программного обеспечения (далее - ПО) и ТС ИС, приводящие к модификации, блокированию, уничтожению, нарушению правил эксплуатации персонального компьютера;

- стихийные бедствия, техногенные аварии, сбои и отказы ТС ИС.

3. Организация работы с ключами от режимных помещений и металлических хранилищ

3.1. Для достижения основной цели защиты информации средства автоматизации и средства защиты информации обеспечивают эффективное решение следующих задач:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;
- своевременное обнаружение фактов несанкционированного доступа;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- недопущение воздействия на ТС обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением защищенности информации;

3.2. Выполнение требований Положения в школы предполагает организацию деятельности школы в соответствии со следующими инструкциями:

- по проведению антивирусного контроля;
- по организации парольной защиты;
- по организации технического обслуживания;
- по работе пользователей в ИС;
- по организации резервного копирования информации.

3.3. Охрана помещений, в которых ведется обработка информации, и организация режима безопасности в этих помещениях должна обеспечивать сохранность ТС ИС, носителей информации и средств защиты информации, исключение возможности неконтролируемого пребывания посторонних лиц в этих помещениях.

4. Обязанности пользователей ИС, ответственных за проведение мероприятий по защите информации

4.1. АИБ и программисты школы:

- сопровождают функционирование программного обеспечения рабочих станций ИС;
- организуют техническое обслуживание рабочих станций, периферийного и другого специализированного оборудования;
- организуют работы по проведению антивирусного контроля рабочих станций;
- отвечают за соблюдение в ИС требований по обеспечению безопасности информации;
- отвечают за своевременное обнаружение фактов несанкционированного доступа к ИС;
- разрабатывают предложения по дальнейшему совершенствованию системы защиты информации, планирует мероприятия по защите ИС.

4.2. Пользователь ИС - сотрудник, допущенный к работе в ИС:

- отвечает за соблюдение установленного порядка использования ПО, применение технических и программных средств ИС;
- соблюдает требования нормативных документов по обеспечению безопасности информации, обрабатываемой ИС;
- обеспечивает исключение возможности изменения компонентов персонального компьютера, отключение или изменение настроек антивирусной защиты.

5. Ответственность

5.1. Ответственность за реализацию и соблюдение требований Положения пользователями ИС возлагается на пользователей ИС школы.

5.2. Нарушение требований Положения влечет за собой дисциплинарную, административную и иную ответственность в соответствии с действующим законодательством Российской Федерации.