Государственное бюджетное дошкольное образовательное учреждение
детский сад № 103
Центрального района Санкт-Петербурга

ПРИНЯТО
Общим собранием работников
ГБДОУ № 103
Центрального района СПб
Протокол № 1 от 28.08.2020г.

УТВЕРЖДАЮ
Заведующий ГБДОУ №103
Центрального района СПб
_____Е. В. Мальцева
Приказ № 27от 01.09.2020г.

ГБДОУ №103Центрального района Санкт-Петербурга
Подписано цифровой подписью: ГБДОУ №103Центрального района Санкт-Петербурга
Дата: 2021.04.08 17:25:27 +03'00'

Положение
об информационной безопасности

Государственного бюджетного дошкольного образовательного учреждения
детского сада № 103
Центрального района Санкт-Петербурга

г. Санкт-Петербург
2020

1. Общие положения

1.1. Положение об информационной безопасности (далее по тексту – Положение) Государственного бюджетного дошкольного образовательного учреждения детского сада №103 Центрального района Санкт-Петербурга (далее по тексту – ДОУ) определяет организацию, осуществление и контроль мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ДОУ.

1.2. Положение разработано в соответствии с Федеральным законом от 29.12.2012 года №273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 7 октября 2017 года №1235 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности этих объектов (территорий)», с целью осуществления мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ДОУ.

1.3.Для обеспечения информационной безопасности ДОУ, приказом заведующего ДОУ назначаются ответственные лица за обеспечение информационной безопасности ДОУ, которые в своей работе руководствуются данным Положением.

1.4. Положение принимается решением Общего собрания работников ДОУ, с учетом мнения профсоюзного комитета первичной профсоюзной организации ДОУ, утверждается приказом заведующего ДОУ. Изменения и дополнения в настоящее Положение вносятся решением Общего собрания работников ДОУ, с учетом мнения профсоюзного комитета первичной профсоюзной организации ДОУ, утверждаются приказом заведующего ДОУ.

1.5. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

2. Цели и задачи информационной безопасности ДОУ

2.1. Цель: осуществление мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ДОУ.

2.2. Основными задачами обеспечения информационной безопасности являются:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализация права на доступ к информации;
- организация эксплуатации технических и программных средств защиты информации. Текущий контроль работы средств и систем защиты информации;
- организация и контроль резервного копирования информации.

3. Ответственные лица за обеспечение информационной безопасности ДОУ

3.1. Ответственные лица за обеспечение информационной безопасности (далее по тексту – ответственные лица) в пределах своих функциональных обязанностей обеспечивают безопасность информации обрабатываемой, передаваемой и хранимой при помощи информационных средств в ДОУ.

3.2. Ответственные лица за информационную безопасность выполняют следующие основные функции:

- разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете;

- обучение работников-пользователей персональных компьютеров (далее по тексту - ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации;

- организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ;

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;

- контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём;

- контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;

- контроль пользования Интернетом.

4. Обязанности ответственных лиц за обеспечение информационной безопасности ДОУ

4.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей. Немедленно докладывать заведующему ДОУ о выявленных нарушениях и несанкционированных действиях работников-пользователей ПК, а также принимать необходимые меры по устранению нарушений, выявленных нарушениях и несанкционированных действиях работников-пользователей ПК, а также принимать необходимые меры по устранению нарушений.

4.2. Совместно с программистами обслуживающих ДОУ организаций (при наличии контракта, договора и т.д.), принимать меры по восстановлению работоспособности средств и систем защиты информации.

4.3. Проводить инструктаж работников-пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

4.4. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

4.5. Контролировать регулярное резервное копирование данных (не реже чем один раз в неделю) всеми пользователями ПК, иметь возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

4.6. Предотвращать несанкционированный доступ к информации и (или) передачи ее лицам, не имеющим права на доступ к информации.

4.7. Своевременно выявлять факты несанкционированного доступа к информации.

4.8. Предупреждать возможности неблагоприятных последствий нарушения порядка доступа к информации.

4.9. Не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

4.10. Постоянно контролировать обеспечение высокого уровня защищенности информации в ДОУ.

5. Права ответственных лиц за обеспечение информационной безопасности ДОУ

5.1. Требовать от работников-пользователей ПК безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения.

5.2. Готовить предложения по совершенствованию системы информационной

безопасности ДОУ.

6. Ответственность ответственных лиц за информационную безопасность ДОУ

6.1. На ответственных лиц за информационную безопасность ДОУ возлагается персональная ответственность за качество проводимых ими работ по обеспечению информационной безопасности ДОУ, защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением.