ПРИНЯТО
Общим собранием работников
ГБДОУ № 9 Калининского района
Санкт-Петербурга
протокол от 25.01.2022 № 02

УТВЕРЖДАЮ
Заведующий ГБДОУ № 9
Калининского района Санкт-Петербурга
Приказ от 26.01.2022 № 06/1-А
_____Ж.Л.Пакалюк

ПОЛОЖЕНИЕ
об информационной безопасности

Государственного бюджетного дошкольного образовательногоучреждения детского сада № 9 общеразвивающего вида с приоритетным осуществлением деятельности по физическому развитию детей Калининского района
Санкт-Петербурга

Санкт-Петербург
2022

1. Общие положения.

Положение об информационной безопасности государственного бюджетного дошкольного образовательного учреждения детского сада №9 общеразвивающего вида с приоритетным осуществлением деятельности по физическому развитию детей Калининского района Санкт-Петербурга, (далее - Положение) разработано в соответствии с Федеральным законом № 273-ФЗ от 29.12.2012 г. «Об образовании в Российской Федерации», Федеральным законом № 152- ФЗ от 27.07.2006 г.(с изменениями на 02.07.2021 г.) «О персональных данных», Федеральным законом Российской Федерации от 27.07.2006 года N 149-ФЗ (с изменениями на 30.12.2021 г.) «Об информации, информационных технологиях и о защите информации», Письмом Федерального агентства по образованию от 29.07.2009 г. № 17-110 «Об обеспечении защиты персональных данных». Письмом Министерства образования и науки РФ от 13.08.2002 г. N 01- 51-088ин «Об организации использования информационных и коммуникационных ресурсов в общеобразовательных учреждениях», Постановлением Правительства Российской Федерации от 17.11.2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

В понятие информационной безопасности образовательного учреждения входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы, защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

В составе массивов охраняемой законом информации, находящейся в распоряжении образовательного учреждения, можно выделить три группы:

- персональные сведения, касающиеся воспитанников и сотрудников, оцифрованные архивы;
- ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;
- структурированная информация, обеспечивающая воспитательно-образовательный процесс (библиотеки, базы данных, обучающие программы).

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизированного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц.

2. Угрозы информационной безопасности.

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и деятельность сотрудников, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус.

Группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

- компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;
- программы, используемые для обеспечения работоспособности системы или в воспитательно-образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
- данные, хранимые как на жестких дисках, так и на отдельных носителях;
- сам персонал, отвечающий за работоспособность IT-систем;
- взрослые, подверженные внешнему агрессивному информационному влиянию и способные создать в ГБДОУ криминальную ситуацию.

Угрозы, направленные на повреждение любого из компонентов системы, не зависящие от намерения персонала, учащихся или третьих лиц:

- любые аварийные ситуации, например, отключение электроэнергии или затопление;
- ошибки персонала;
- сбои в работе программного обеспечения;
- выход техники из строя;
- проблемы в работе систем связи.

3. Способы несанкционированного доступа.

Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. При наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

Аппаратный способ связан с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

4. О системном администрировании и обязанностях ответственного за информационную безопасность.

Задачи связанные с мерами системного администрирования, обеспечивающего информационную безопасность являются частью работы ответственного за информационную безопасность по обслуживанию компьютерной техники Учреждении.

Для решения задач информационной безопасности ответственный за информационную безопасность должен:

Следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.)

Обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи.

Обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей.

Обеспечивать нормальное функционирование системы резервного копирования.

5. Базы данных.

Базы данных подлежащие защите вносятся в «Реестр баз данных подлежащих информационной защите».

Все процедуры по использованию и обслуживанию базы данных осуществляет ответственный за ведение базы данных. В том числе:

- резервное копирование;
- периодический контроль исправности резервных копий;
- подключение и отключение пользователей;
- внесение изменений в структуру базы, а также изменений в «Реестр баз данных подлежащих информационной защите», при необходимости (изменение степени конфиденциальности, места расположения и т.д.); прочие виды работ связанных с данной базой.

В случае если база данных требует парольной защиты, то ответственный за базу данных руководствуется требованиями раздела 6 «Система аутентификации» настоящего документа.

6. Система аутентификации.

На всех ПК используется WINDOWS XP PROFESSIONAL, WINDOWS 7, WINDOWS 8.

Для всех пользователей базы данных устанавливаются уникальные пароли. Периодичность плановой смены паролей 1 раз - в начале учебного года. Устанавливается блокировка учетной записи пользователей при неправильном наборе пароля более пяти раз.

Устанавливается блокировка экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 30 мин., с последующим вводом пароля для разблокирования ПК.

Пользователи обязаны осуществлять выход из базы данных, если планируется отсутствие на рабочем месте более 1,5 часов.

Пользователи обязаны не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.

Обслуживание системы аутентификации осуществляютответственные за базы данных.

7. Защита по внешним цифровым линиям связи.

В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через компьютеры с установленными брэндмауэром и антивирусом.

Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.

Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гатжетов) к сети WiFi ГБДОУ №9.

8. Защита от несанкционированного подключения и размещение активного сетевого оборудования.

Сервер учреждения размещается в кабинете заедующего при отсутствии специально выделенной серверной.

Доступ к серверу ограничен паролем, который известен только ответственному за информационную безопасность, ответственному за информатизацию.

Роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

9. Процедура увольнения сотрудников имеющих доступ к сети.

В случае кадровых перестановок и изменений все ответственные за базы данных переназначаются приказомЗаведующего, новым сотрудникам предоставляются логины и пароли для доступа к базам данных.

10. Антивирусная защита.

На основании Правил пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.) не допускается работа без организации антивирусной защиты. Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

За своевременное обновление антивирусного программного обеспечения отвечает ответственный за информационную безопасность.

11.Заключительные положения

Настоящее Положение является локальным нормативным актом ГБДОУ, принимается на Общем собрании работников и утверждается приказом заведующего ГБДОУ.

Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

Поле принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 603332450510203670830559428146817986133868575820

Владелец Пакалюк Жанна Леонидовна

Действителен С 14.04.2022 по 14.04.2023