ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00EC17A493F0B1BBF11B924AA3B14750D4
Владелец: Прокашева Любовь Николаевна
Действителен: с 13.01.2025 до 08.04.2026

Утверждено
Директор МБОУ «Красногорская СОШ»
_____Л.Н.Прокашева
Приказ № 19/01 осн. от «06.03»2025 г.

Положение

об информационной безопасности МБОУ «Красногорская СОШ»

1.Общие положения

1.1.Информационная безопасность является одним из составных элементов комплексной безопасности в Муниципальном бюджетном образовательном учреждении «Красногорская СОШ» (далее-Школа), порядок организации по ее созданию и функционированию.
1.2. Данное положение разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Трудовым кодексом РФ от 30.12.2001№ 197-ФЗ (с изм. и доп.), Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и имеет статус локального нормативного акта образовательной организации. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.
1.3.Под информационной безопасностью Школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а так же прав субъектов информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локацизацию и ликвидацию.
1.4.Использовании сети Интернет в образовательной организации подчинено следующим принципам:
-соответствие образовательным целям;
-способствование гармоническому формированию и развитию личности;
-уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;
-приобретение новых навыков и знаний;
-расширение применяемого спектра учебных и наглядных пособий;
-социализация личности, введение в информационное общество.
1.5.К объектам информационной безопасности в Школе относится:
-информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных; в т.ч. персональные данные;
-средства и системы информатизации – средства вычислительной и организационной техники, локальной сети; общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отражения информации.

1.6.Система информационной безопасности (далее-СПБ) должна обязательно обеспечивать:
-конфиденциальность (защиту от несанкционированного раскрытия или перехвата);
-целостность (точность и полноту информации и компьютерных программ);
-доступность (возможность получения пользователями информации в пределах их компетенции).
1.7.Обеспечение информационной безопасности осуществляется по следующим правилам:
-правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
-организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-нибудь ущерба;
-инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

2.Цели и задачи обеспечения безопасности информации

2.1.Главной целью обеспечения безопасности информации, циркулирующей в Школе, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту – конфиденциальной или защищаемой информации) и предотвращения ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Школы.
2.2.Основными целями обеспечения безопасности информации являются:
-предотвращения утечки, хищения, искажения, подделки информации, циркулирующей в Школе;
-предотвращение нарушений прав личности обучающихся, работников Школы на сохранение конфиденциальности информации;
-предотвращение несанкционированных действий по блокированию информации.
2.3.Основными задачами обеспечения безопасности информации являются:
-соответствие положениями законодательных актов и нормативным требованиям по защите информации;
-своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интереса Школы, нарушению нормального функционирования и развития Школы ;
-создание механизма оперативного реагирования на угрозы информационной безопасности и негативных тенденций в системе информационных отношений;
-эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
-развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
-развитие и совершенствование защищенного юридически значимого электронного документооборота;

-создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований
-создание механизмов управления системой информационной безопасности.

3.Правовые нормы обеспечения информационной безопасности

3.1.Школа имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.
3.2.Школа обязана обеспечить сохранность конфиденциальной информации.
3.3.Администрация школы:
-издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизма их защиты;
-имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
-имеет право включать требования по защите информации в договоры по всем видам деятельности;
-разрабатывать перечень сведений конфиденциального характера;
-имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.
3.4.Организационные и функциональные документы по обеспечению информационной безопасности:
-приказ директора о назначении ответственного за обеспечение информационной безопасности;
-должностные обязанности ответственного за обеспечение информационной безопасности;
-перечень защищаемых информационных ресурсов и баз данных.
3.5.Порядок допуска сотрудников Школы к информации предусматривает:
-принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
-ознакомление работника с нормами законодательства РФ и Школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
-ознакомление работников специалистом по информационной безопасности;
-контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

4.Использование сети Интернет

4.1.Использование сети Интернет в Школе осуществляется в целях образовательного характера. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.
4.2.Работники Школы вправе:
-размещать информацию в сети Интернет на интернет-ресурсах Школы.

4.3.работникам Школы запрещено размещать в сети Интернет и на образовательных ресурсах информацию:
-противоречащую требованию законодательства РФ и локальным нормативным актам Школы;
-не относящуюся к образовательному процессу и не связанную с деятельностью Школы;
-нарушающую нравственные и этические нормы, требования профессиональной этики.
4.4.Обучающиеся Школы вправе:
-использовать ресурсы, размещать в сети Интернет, в том числе интернет-ресурсы Школы, в порядке и на условиях, которые предусмотрены настоящим Положением.
4.5.Обучающимся запрещено:
-находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и/или нарушают законодательство РФ;
-осуществлять любые сделки через интернет;
-загружать файлы на компьютер Школы без разрешения ответственного лица;
-распространять оскорбительную, не соответствующую деятельности, порочащую других лиц информацию, угрозы.
4.6.Запред и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает ответственное лицо, назначенное приказом директора Школы.
4.7.Если в процессе работы пользователем будет обнаружен ресурс, содержимого которого не совместимо с целями образовательного процесса, он обязан немедленно сообщить ответственному лицу с указанием интернет-адреса (URL) И покинуть данный ресурс.
4.8.Ответственное лицо обязано:
-принять сообщение пользователя;
-принять меры по отключению выхода на данный ресурс с интернет-ресурсов Школы;
-если обнаруженный ресурс явно нарушает законодательство РФ – сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством РФ (в течении суток).
Передаваемая информация должна содержать:
-интернет-адрес (URL) ресурса;
-тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;
-дату и время обнаружения;
-информацию об установленных в образовательной организации технических средствах доступа к информации.

5.Мероприятия по обеспечению информационной безопасности

5.1.Для обеспечения информационной безопасности в Школе требуется проведение следующих первоочередных мероприятий:
-защита интеллектуальной собственности Школы;
-защита компьютеров, локальных сетей и сети подключения к системе Интернета;
-организация защиты конфиденциальной информации, в т.ч. персональных данных работников и обучающихся школы;
-учет всех носителей конфиденциальной информации.

6.Организация работы с информационными ресурсами и технологиями

6.1.Система организации делопроизводства:
-учат документов Школы, в том числе и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
-регистрация и учет всех входящих (исходящих) документов Школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т.д.);
-особый режим уничтожения документов.
6.2.В ходе использования, передачи копирования и исполнения документов также необходимо соблюдать определенные правила.

7.О системном администрировании и обязанностях ответственного за информационную безопасность

7.1.Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы ответственного зха информацию в Школе.
7.2.Для решения задач информационной безопасности ответственный за информатизацию обязан:
-следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей один раз в квартал и по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и др.);
-обеспечить функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
-обеспечить мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
-обеспечивать нормальное функционирование системы резервного копирования.

8.Анитивирусная защита.

Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.)
8.1.Основным способом проникновения компьютерных ресурсов на компьютере пользователя в настоящее время является Интернет и электронная почта. В связи с этим компьютерах, используемых обучающимися в учебной деятельности, устанавливается программное обеспечение, блокирующее доступ к негативной информации, которое обеспечено провайдером и программной поддержкой браузера (фильтр-контент);
8.2.Обучающимся закрыт доступ к сети Интернет через Wi-fi в местах общего пользования школы (библиотеки, коридоры и учебные кабинеты) с помощью пароля и прокси-сервера;
8.3.Исключена возможность установки на школьные компьютеры игр и другого ПО не связанных с образовательным процессом. Обучающиеся работаю за компьютерами исключительно в присутствии и под руководством педагогов;
8.4.Мониторинг качества системы контентной фильтрации в Школе проводится ежедневно.