Государственное бюджетное общеобразовательное учреждение Ленинградской области «Лужская школа-интернат, реализующая адаптированные образовательные программы»

(ГБОУ ЛО «Лужская школа-интернат»)

«СОГЛАСОВАНО» с представительным органом работников ОУ	«РАССМОТРЕНО» на собрании трудового коллектива (протокол от 26.03.2021 № 28)	«УТВЕРЖДЕНО» распоряжением ГБОУ ЛО «Лужская школа-интернат» от 31.03.2021 № 178/1

Регистрационный номер_179/39_

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сведения о сертификате ЭП
Сертификат: 39E3 B37E 0000 0000 E26A
Владелец: Кудрявцева Марина Александровна
Срок действия: с 25 ноября 2021 г. 11:03:18 по 25 февраля 2023 г. 11:13:18

Положение о информационной безопасности

Доведено до сведения обучающихся _01.04.2021_	Доведено до сведения родителей (законных представителей) _02.04.2021_

Луга
2021

Общие положения

1. Настоящее положение Государственного бюджетного общеобразовательного учреждения Ленинградской области «Лужская школа-интернат, реализующая адаптированные образовательные программы» регулирует вопросы Информационной безопасности. Информационная безопасность является одним из составных элементов комплексной безопасности.

1.2. Настоящее положение разработано на основании с ТК РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.), Федеральный законом от 07.07.2003 № 126-ФЗ «О связи», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации"», Федеральным законом от 27.07.2006 № 152-ФЗ (в ред. От 27.07.2011) «О персональных данных», Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности».

1.3 Настоящее положение является обязательным для всех участников образовательных отношений, для работников ОУ, обучающихся их родителей (законных представителей)

Информационная безопасность является одним из составных элементов комплексной безопасности. Под информационной безопасностью ГБ ОУ ЛО «Лужская школа-интернат» (далее – Учреждения) следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

К объектам информационной безопасности в Учреждении относятся:

• информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

• информация, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;

• средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

Система информационной безопасности должна обязательно обеспечивать:

• конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

• целостность (точность и полноту информации и компьютерных программ);

• доступность (возможность получения пользователями информации в пределах их компетенции).

Обеспечение информационной безопасности осуществляется по следующим направлениям:

• правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
• организационная защита - это регламентация деятельности Учреждения и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба
• инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Цели и задачи обеспечения безопасности информации

Главной целью обеспечения безопасности информации, циркулирующей в Учреждении, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды Учреждения
. 2.2. Основными целями обеспечения безопасности информации являются:
• предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в Учреждении;
• предотвращение нарушений прав личности обучающихся, работников Учреждения на сохранение конфиденциальности информации;
• предотвращение несанкционированных действий по блокированию информации.
2.3. Основными задачами обеспечения безопасности информации являются:
• соответствие положениям законодательных актов и нормативным требованиям по защите информации;
• своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам Учреждения, нарушению нормального функционирования и развития Учреждения;
• создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции 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 информационной безопасности;
• создание механизмов управления системой информационной безопасности.

3. Правовые нормы обеспечения информационной безопасности

Учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Учреждения, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

Учреждение обязано обеспечить сохранность конфиденциальной информации.

Администрация Учреждения:

• назначает ответственного за обеспечение информационной безопасности;
• имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
• имеет право включать требования по защите информации в договоры по всем видам деятельности;
• разрабатывает перечень сведений конфиденциального характера;
• имеет право требовать защиты интересов Учреждения со стороны государственных и судебных инстанций.

Организационные и функциональные документы по обеспечению информационной безопасности:

• приказ директора Учреждения о назначении ответственного за обеспечение информационной безопасности;
• перечень защищаемых информационных ресурсов и баз данных;
• инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Учреждения и др.

Порядок допуска сотрудников Учреждения к информации предусматривает:

• принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
• ознакомление работника с нормами законодательства РФ и Учреждения об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
• инструктаж работника по информационной безопасности
• контроль работника при работе с информацией конфиденциального характера.

4. Организация системы обеспечения информационной безопасности

В целях реализации стоящих перед системой обеспечения информационной безопасности задач в Учреждении устанавливаются:

• защита интеллектуальной собственности Учреждения;
• защита компьютеров, локальных сетей и сети подключения к системе Интернета;
• организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Учреждения;
• учет всех носителей конфиденциальной информации;
• контроль за использованием электронных средств информационного обеспечения деятельности Учреждения по прямому назначению;
• противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности Учреждения нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;
• принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;
• обучение персонала Учреждения по вопросам обеспечения информационной безопасности;
• контроль за правильностью использования имеющихся в Учреждении средств телефонной и радиосвязи.

5. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Для обеспечения информационной безопасности в образовательной организации 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

Для организации делопроизводства приказом директора Учреждения назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором Учреждения.

Система организации делопроизводства:
• учет всей документации Учреждения, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
• регистрация и учет всех входящих (исходящих) документов Учреждения в специальном журнале информации о дате получения (отправления)

документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

• регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

• особый режим уничтожения документов.

В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

Запрещается выносить документы с грифом «Для служебного пользования» за пределы Учреждения.

При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

Всѐ программное обеспечение устанавливается только зам. директора по АХЧ.