Муниципальное автономное общеобразовательное учреждение
средняя общеобразовательная школа с углубленным изучением отдельных предметов № 2
г. Туймазы муниципального района Туймазинский район
Республики Башкортостан

Согласовано
Совет обучающихся
МАОУ СОШ № 2 г. Туймазы
Протокол № 1 от 27.08.2020

Согласовано
Совет родителей
МАОУ СОШ № 2 г. Туймазы
Протокол № 1 от 27.08.2020

Согласовано
Педагогический совет
МАОУ СОШ № 2 г. Туймазы
Протокол № 1 от 28.08.2020

Утверждаю
И.о. директора МАОУ СОШ №2 г.Туймазы
_____ /И.В. Тимофеева./
приказ №188 от 28.08.2020

Моисеева Елена Николаевна

Подписано цифровой подписью: Моисеева Елена Николаевна
Дата: 2021.09.17 21:37:22 +05'00'

ПОЛОЖЕНИЕ
об информационной безопасности

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности. Под информационной безопасностью МАОУ СОШ №2 г. Туймазы (далее – ОО) 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.

1.2. Данное положение разработано в соответствии с 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".

1.3. К объектам информационной безопасности в ОО 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.

1.4. 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).

1.5. 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 ОО 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

2.1. Главной целью обеспечения безопасности информации, циркулирующей в ОО, 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 ОО.
2.2. Основными целями обеспечения безопасности информации являются:
• предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в ОО;
• предотвращение нарушений прав личности обучающихся, работников ОО 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 ОО, нарушению нормального функционирования и развития ОО я;
• 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

3.1. ОО имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников ОО, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.
3.2. ОО обязана обеспечить сохранность конфиденциальной информации.
3.3. Администрация ОО:
• 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 ОО со стороны государственных и судебных инстанций.

3.4. Организационные и функциональные документы по обеспечению информационной безопасности:
• приказ директора ОО 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 ОО и др.
3.5. Порядок допуска сотрудников ОО к информации предусматривает:
• принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
• ознакомление работника с нормами законодательства РФ и ОО об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
• инструктаж работника специалистом по информационной безопасности;
• контроль работника ответственным за информационную безопасность, при работе с информацией конфиденциального характера.

3.6 Использование сети Интернет

3.6.1. Использование сети Интернет в Школе осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.
3.6.2. ***Работники вправе:***
• размещать информацию в сети Интернет на интернет-ресурсах ОО;
• иметь учетную запись электронной почты на интернет-ресурсах
3.6.3. ***Работникам запрещено*** размещать в сети Интернет и на образовательных ресурсах информацию: «противоречащую требованиям законодательства РФ и локальным нормативным актам ОО; не относящуюся к образовательному процессу и не связанную с деятельностью ОО, нарушающую нравственные и этические нормы, требования профессиональной этики.
3.6.4. ***Обучающиеся вправе:***
• использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Школы, в порядке и на условиях, которые предусмотрены настоящим Положением.
• размещать информацию и сведения на интернет-ресурсах ОО.
3.6.5 ***Обучающемся запрещено:***
- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство РФ;
- в осуществлять любые сделки через интернет;
- загружать файлы на компьютер ОО без разрешения ответственного лица;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.
3.6.6 Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора ОО.
3.6.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом ответственному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс. Ответственное лицо должно зафиксировать в «Журнал регистрации случаев обнаружения сайтов, не соответствующие задачам образования».

4. Организация системы обеспечения информационной безопасности

4.1. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в ОО устанавливаются:
• защита интеллектуальной собственности ОО;
• защита компьютеров, локальных сетей и сети подключения к системе Интернета с контентной фильтрацией от провайтера;

• организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся ОО;
• учет всех носителей конфиденциальной информации;
• контроль за использованием электронных средств информационного обеспечения деятельности ОО по прямому назначению;
• противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности ОО 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 ОО по вопросам обеспечения информационной безопасности;
• контроль за правильностью использования имеющихся в ОО средств телефонной и радиосвязи.

5. Организация работы с информационными ресурсами и технологиями

5.1. Для организации делопроизводства приказом директора ОО назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором ОО. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.
5.2. Система организации делопроизводства:
• учет всей документации ОО, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
• регистрация и учет всех входящих (исходящих) документов ОО 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.
5.3. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:
5.3.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
5.3.2. 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.
5.3.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.
5.3.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.
5.3.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы ОО.
5.3.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.
5.4. Всѐ программное обеспечение устанавливается только с разрешения ответственного за информационную безопасность.
5.5 Срок данного Положения не ограничен. Данное Положение действует до принятия нового.