Муниципальное автономное общеобразовательное учреждение
«Средняя школа № 1»
Петропавловск - Камчатского городского округа

Рассмотрено	«Утверждаю»
на заседании педагогического совета школы	Директор МАОУ «Средняя школа № 1»
Протокол № ___	_____ С.В. Беликов
«___»_____ 20___г.	«___»_____ 20___г.

Беликов Сергей Викторович подтверждаю этот документ своей удостоверяющей подписью 00e8459c2679634583f85c87aeac55ecb7 2023.04.17 14:32:19+12'00'

ПОЛОЖЕНИЕ № 137
об информационной безопасности

1. Общие положения

Информационная безопасность является одним из составных элементов комплексной безопасности школы.

Под информационной безопасностью школы 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 (защищаемые информационные ресурсы и базы данных) относятся:

- перечень сведений, составляющих государственную тайну, в соответствии с Законом РФ от 21 июля 1993г. №5485-1 «О государственной тайне», утвержденных Указом Президента РФ.
- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и 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 (далее - СИБ) 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 производственной деятельности 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. Правовые нормы обеспечения информационной безопасности

- учреждение имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся, работников школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;

- учреждение обязано обеспечить сохранность конфиденциальной информации;

- учреждение обязано обеспечить запрет на распространение информации, негативно влияющей на несовершеннолетних, запрещенной к распространению в соответствии с Федеральным законом №114-ФЗ от 25 июля 2002 «О противодействии экстремистской деятельности»;

- учреждение обязано обеспечить защиту информационных ресурсов сайта от размещения на них информации несовместимой с целями и задачами образовательного процесса.

Администрация учреждения:

- назначает ответственного за обеспечение информационной безопасности;

- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы 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;

- разрабатывает перечень сведений конфиденциального характера;

- имеет право требовать защиту интересов учреждения со стороны государственных и судебных инстанций.

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;

- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников учреждения и др.

Кроме того, должен быть определен порядок допуска сотрудников учреждения к информации. Такой допуск 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 специалистом по информационной безопасности;

- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности

3.1. Для обеспечения информационной безопасности в учреждении требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности учреждения;

- защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся учреждения;

- учет всех носителей конфиденциальной информации.

3.2. Обладатель информации обязан обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением уровня защищенности информации.

4. Организация работы с информационными ресурсами и технологиями

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:

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

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.

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

4. Передача документов исполнителю производится только через канцелярию или ответственного за организацию делопроизводства.

Запрещается выносить документы с грифом "Для служебного пользования" за пределы учреждения.

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

Для организации делопроизводства приказом директора назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. Нормативные документы

Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.).

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».