ПРИНЯТО
Педагогическим советом
Протокол от 22.05.2019 № 12

УТВЕРЖДЕНО
Приказом МБОУ СОШ № 11
от 22.05.2019 № 02-01-264

Положение об информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 11»

1. Общие положении

1.1. Настоящее Положение об информационной безопасности Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа № 11» (далее – Положение) разработано в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Закон об образовании в Российской Федерации»;
- 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 защите персональных данных»;
- Постановлением Правительства РФ от 7 октября 2017 года № 1235 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»;
- Положением о порядке обращения со служебной информацией ограниченного распространений, утвержденного Постановлением Правительства РФ от 3 ноября 1994 года № 1233.

1.2. Положение определяет порядок обеспечения информационной безопасности в Муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа № 11» (далее – Школа).

1.3. Под информационной безопасностью Школы понимается 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.

1.4. К объектам информационной безопасности в Школе относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера, информацию, 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.

1.5. 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).

2. Обеспечение информационной безопасности

2.1. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе:

- организационная зашита – 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.

2.2. Систему обеспечения информационной безопасности можно разбить на следующие подсистемы:

- компьютерная безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

2.3. Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

2.4. Безопасность данных достигается защитой данных от неавторизованных, случайных, умышлённых или возникших по халатности модификаций или разглашения.

2.5. Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

2.6. Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

2.7. К объектам информационной безопасности Школы относятся:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, к конфиденциальной информации, представленную в виде документированных информационных массивов и баз данных;
- средства и системы информатизации – средства вычислительной организационной техники сети и системы, общесистемное и прикладное программное обеспечение, авторизованные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора,

регистрации, передачи, обработки и отображения информации, а также их информационные физические поля.

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. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Школы о назначении ответственного за антитеррористическую безопасность;
- приказ директора Школы о назначении ответственного за обеспечение информационной безопасности;
- приказ директора школы о назначении ответственного за хранение документов, содержащих информацию ограниченного распространения;
- приказ директора Школы о защите служебной информации и информационных ресурсов;
- должностные обязанности ответственного за антитеррористическую безопасность;
- должностные обязанности ответственного за обеспечение информационной безопасности.

3.4. К документам, содержащим служебную информацию ограниченного распространения, допускаются работники Школы только на основании приказа директора школы.

3.5. Контроль за работой с документами, содержащими служебную информацию ограниченного распространения, осуществляет ответственный за антитеррористическую безопасность Школы.

3.6. Контроль за ведением сайта Школы и обеспечением защиты информационных ресурсов осуществляет ответственный за обеспечение информационной безопасности Школы.

3.7. 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.

4. Организация работы с информационными ресурсами

4.1. Система организации делопроизводства:

4.1.1. учет всей документации школы, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

4.1.2. 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.);

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

4.2. Документы, содержащие информацию ограниченного распространения, и личные дела должны храниться в служебном помещении. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

4.3.Выданные для работы документы запрещается выносить за пределы Школы и подлежат возврату в тот же день.

4.4. Передача документов, содержащих информацию ограниченного распространения, исполнителю производится только через ответственного за хранение данных документов.