

МБОУ «Средняя общеобразовательная школа №12» г. Калуги

Принято
на заседании педагогического совета
Протокол № 4 от 02.02.2024 г.



Положение об обеспечении информационной безопасности

Калуга

Положение

об обеспечении информационной безопасности

1. Общие положения

- 1.1. Настоящее Положение об обеспечении информационной безопасности в МБОУ «Средняя общеобразовательная школа №12» г. Калуги (далее - Положение) определяет систему правовых, организационных и технических мероприятий, направленных на обеспечение информационной безопасности обучающихся и работников школы.
- 1.2. Положение разработано в соответствии с:
 - Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
 - Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационн[^]х технологиях и о защите информации»;
 - Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данн[^]х»;
 - Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - Доктриной информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646;
 - Концепцией информационной безопасности детей, утв. Распоряжением Правительства РФ от 02.12.2015 № 2471-р;
 - Методическими рекомендациями о размещении на информационн[^]х стендах, официальн[^]х интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет, направленными Письмом Минобрнауки России от 14.05.2018 № 08-1184;
 - Уставом МБОУ «Средняя общеобразовательная школа №12» г. Калуги (далее Школа)
- 1.3. Под информационной безопасностью Школы следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационно й деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию
- 1.4. Система информационной безопасности является неотъемлемой частью системы комплексной безопасности Школы.
- 1.5. Функционирование системы информационной безопасности в Школе обеспечивается применением комплекса правовых, организационных и технических мер защиты, в результате чего снижается или исключается риск, связанный с причинением информационной продукцией, используемой в образовательной деятельности, вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию несовершеннолетних обучающихся.
- 1.6. Использование сети Интернет в образовательной деятельности допускается только при условии применения административных и организационных мер, технических (программных, программно-аппаратных) средств защиты обучающихся от информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей.

2. Основные цели и задачи функционирования системы информационной безопасности

- 2.1. Система информационной безопасности направлена на защиту единого информационного образовательного пространства Школы от незаконного проникновения, на предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в локальных сетях, а также недопущения доступа обучающихся и работников учреждения к информации, которая запрещена или ограничена к распространению в Российской Федерации.
- 2.2. Система информационной безопасности Школы направлена на решение следующих задач:
 - 2.2.1. защита прав и законн[^]х интересов обучающихся в образовательной деятельности, защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию и (или) не

- соответствующей задачам образования;
- 2.2.2. разграничение объемов и содержания информации, которая может быть доступна различным категориям пользователей;
 - 2.2.3. предотвращение утечки, хищения, утраты, подделки информации Школы;
 - 2.2.4. предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации учреждения;
 - 2.2.5. предотвращение других форм незаконного вмешательства в информационные ресурсы учреждения и его локальную сеть.
- 2.3. **Объекты информационной безопасности:**
- Информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
 - Информация, защита которой предусмотрена законодательными актами РФ, в том числе персональные данные;
 - Средства и системы информатизации - средства вычислительной и организационной техники в компьютерных классах, локальные сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами в учебных кабинетах, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации

3. Организационно-административные меры, направленные на защиту детей от информации, причиняющей вред их здоровью и (или) развитию, а также не соответствующей задачам образования.

- 3.1. Приказом директора в Школе назначается лицо, ответственное за обеспечение информационной безопасности. В обязанности ответственного за обеспечение информационной безопасности в том числе входит:
- 3.1.1. контроль функционирования системы контентной фильтрации;
 - 3.1.2. контроль функционирования антивирусной защиты, поддержание в актуальном состоянии антивирусных баз автоматической проверке ПК, локальной сети и внешних носителей на наличие вирусов;
 - 3.1.3. контроль соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ персональных компьютеров в том числе в компьютерных классах;
 - 3.1.4. оценка рисков информационной безопасности учреждения;
 - 3.1.5. выявление угроз безопасности оборудованию и локальной сети Школы;
 - 3.1.6. проведение инструктажа работников Школы по правилам работы с используемыми аппаратно-программными средствами и осуществление контроля за действиями пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования;
 - 3.1.7. информирование обучающихся, родителей несовершеннолетних обучающихся, работников Школы о порядке использования сети Интернет и контроль за использованием сети Интернет обучающимися и работниками.
- 3.2. В Школе оказывается организационная и методическая поддержка работникам в области безопасной работы с информационными ресурсами, информационными образовательными технологиями, в том числе, путем их направления на курсы повышения квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет.
- 3.3. В Школе на регулярной основе осуществляется информирование работников, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации, локальных нормативных и организационно-

распорядительных актов Школы по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет».

4. Информация, используемая в образовательной деятельности и контроль за ее содержанием.

- 4.1. Информация и (или) информационная продукция, используемая в образовательной деятельности, осуществляемой в учреждении, должна соответствовать требованиям законодательства Российской Федерации к защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствовать содержанию и задачам образования.
- 4.2. При осуществлении образовательной деятельности в Школе обеспечивается доступ обучающихся и работников к:
 - 4.2.1. печатной продукции, которая входит в библиотечный фонд Школы;
 - 4.2.2. электронным образовательным ресурсам, прошедшим педагогическую экспертизу, рекомендованным и (или) сформированным органами государственной власти, осуществляющими управление в сфере образования, подведомственными им организациями; разработанными издательствами, выпускающими учебную литературу, учреждениями высшего и среднего образования, российскими библиотеками и иными уполномоченными или допущенными органами и организациями;
 - 4.2.3. общедоступным государственным и региональным информационным системам;
 - 4.2.4. информационно-телекоммуникационной сети Интернет;
- 4.3. В работе и (или) общении с обучающимися педагогическим работникам или иным работникам Школы не допускается использовать информацию:
 - 4.3.1. которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иную информацию, за распространение которой предусмотрена уголовная или административная ответственность;
 - 4.3.2. запрещенную для распространения среди детей в соответствии со ст.5 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - 4.3.3. имеющую знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся);
 - 4.3.4. полученную с нарушением авторских или смежных прав;
 - 4.3.5. имеющую конфиденциальный характер в соответствии с действующим законодательством и (или) локальными нормативными актами Школы.
- 4.4. В образовательной и (или) досуговой деятельности с обучающимися, организуемой и проводимой работниками Школы, не допускается посещения зрелищных или иных мероприятий, билеты на которые (афиши или иная информация о мероприятии) содержат знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся).
- 4.5. В процессе осуществления образовательной деятельности с использованием информационно-компьютерных технологий педагогическими работниками осуществляется контроль за использованием обучающимися сети Интернет, в том числе, визуальный контроль.
- 4.6. При обнаружении угроз информационной безопасности Школы, несанкционированного доступа к локальной сети, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники Школы обязаны незамедлительно сообщить об этом руководству для принятия соответствующих мер.
- 4.7. Работник, ответственный за обеспечение информационной безопасности, при получении информации, указанной в п. 4.6. настоящего Положения незамедлительно:
 - 4.7.1. устанавливает обстоятельства получения доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей;
 - 4.7.2. идентифицирует ресурс сети Интернет;

- 4.7.3. в течение 1 (одного) рабочего дня с момента получения информации, указанной в п.4.6. настоящего Положения, проводит мероприятия, направленные на ограничение доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей (вносит изменения в политики доступа, применяемые в технических средствах контентной фильтрации, вносит изменения в конфигурацию технических средств контентной фильтрации, в случае необходимости предпринимает другие меры).
- 4.8. В порядке реагирования на инцидент, угрожающий информационной безопасности Школы и (или) обучающихся и работников Школы, руководством может быть направлено соответствующее сообщение о наличии на страницах сайтов в сети Интернет информации, распространение которой в Российской Федерации запрещено в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также в органы внутренних дел.

5. Организационно-технические мероприятия по формированию безопасных условий доступа обучающихся к ресурсам сети Интернет

- 5.1. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяемым при предоставлении доступа к информации, распространяемой посредством сети Интернет, относятся:
- 5.1.1. средства ограничения доступа к техническим средствам доступа к сети Интернет;
- 5.1.2. средства ограничения доступа к сети Интернет с технических средств третьих лиц;
- 5.1.3. средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети Интернет.
- 5.2. В Школе обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.
- 5.3. Для приобретения и использования программного обеспечения в образовательной и иной деятельности Школы проводится проверка его подлинности.
- 5.4. В Учреждении осуществляется контроль:
- 5.4.1. эксплуатации технических средств контентной фильтрации;
- 5.4.2. организации доступа к сети Интернет в целях исключения возможности несанкционированного использования сети Интернет в Школе;
- 5.4.3. функционирования технических средств, применяемых при организации доступа к сети Интернет, и их конфигурации (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение в компьютерных классах и автоматизированных рабочих местах в учебных кабинетах);
- 5.4.4. функционирования системы антивирусной защиты;
- 5.4.5. наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, путем осуществления попыток получения доступа к таким ресурсам сети Интернет;
- 5.5. В учреждении не допускается обучающимися и работниками, а также иными лицами самовольная установка программного обеспечения на компьютерную технику Школы, либо использование не принадлежащих Школе программ и оборудования.

6. Обучение и просвещение в сфере информационной безопасности

- 6.1. В рамках образовательной деятельности в Школе осуществляется обучение безопасным способам работы в информационно-телекоммуникационных сетях, в план воспитательной работы Школы включаются мероприятия, направленные на повышение медиаграмотности обучающихся, формированию навыков безопасного поведения в сети Интернет.
- 6.2. В Школе проводятся образовательные и консультационные мероприятия с родителями (законными представителями) обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет.
- 6.3. На информационн¹х стендах, расположенных в Школе и в кабинетах, оснащенн¹х персональными устройствами для выхода в сеть Интернет, компьютерных классах размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.
- 6.4. На официальном сайте Школы размещается специализированный раздел «Информационная безопасность», в рамках которого предусмотрено размещение локальных нормативных актов в сфере обеспечения информационной безопасности обучающихся, нормативно-правовых документов, регламентирующих обеспечение информационной безопасности несовершеннолетних, методические рекомендации, информационные памятки для работников, обучающихся и их родителей, направленные на повышение информационной грамотности и обеспечение информационной безопасности детей.

7. Заключительные положения

- 7.1. Положение вступает в силу с момента его утверждения приказом директора Школы.
- 7.2. Положение отменяется или изменяется в случае изменения действующего законодательства, а также при наличии иных нормативно-правовых оснований, влекущих изменение, дополнение или отмену закрепленных в нем положений.
- 7.3. Положение размещается на информационн¹х стендах Школы и на официальном сайте Школы в сети Интернет.