Утверждено
Приказом директора
МБОУ СОШ с. Стародубское
от 15.02. 2024 № 63/1 -ОД

Положение
об информационной безопасности
в МБОУ СОШ с. Стародубское

1. Общие положения

1.1. Положение об информационной безопасности в МБОУ СОШ с. Стародубское (далее по тексту – Положение) разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации", Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ. Гражданским кодексом Российской Федерации от 30.11.1994 №51-ФЗ, Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, постановлением Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности в муниципальном бюджетном общеобразовательном учреждение «Средняя общеобразовательная школа» с. Стародубское (далее — школа), порядок организации работ по её созданию и функционированию.

1.3. Под информационной безопасностью Школы следует понимать состояние защищенности информационных ресурсов, технологий, баз данных, их формирования и использования, а также прав и обязанностей субъектов информационной деятельности. Система информационной безопасности школы направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

2. Цели и задачи обеспечения безопасности информации

2.1. Главной целью обеспечения безопасности информации, ограниченной в обороте, циркулирующей в школе, 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 школы.

2.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в школе;
- предотвращение нарушений прав личности учащихся, работников школы на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

2.3. Основными задачами обеспечения безопасности информации являются:

- соответствие системы обеспечения информационной безопасности школы 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 школы, нарушению нормального функционирования и развития школы;
- 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 эффективных мер обеспечения безопасности персональных данных;
- создание механизмов управления системой информационной безопасности.

3. Основы обеспечения информационной безопасности

3.1. Школа имеет право самостоятельно определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся и их родителей (законных представителей), 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. Администрация школы:

- назначает ответственных лиц за обеспечение информационной безопасности и безопасное функционирование информационной системы школы;
- 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 (при наличии), трудовой договор;
- *имеет право включать требования по защите информации в договоры по всем видам деятельности;*

- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересовшколы со стороны государственных и судебных инстанций;
- организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечивает сохранность носителей персональных данных;
- определяет перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

3.4. Школа устанавливает порядок допуска сотрудников к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и школы 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.

4. Меры по обеспечению информационной безопасности

4.1. Меры по обеспечению безопасности принимаются в школе для защиты информации, доступ к которой ограничен, от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий.

4.2. Основные меры по обеспечению информационной безопасности в школе с учётом актуальных угроз безопасности и применяемых информационных технологий, включают:

- управление доступом к информации;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранится и (или) обрабатываются информация;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

4.3. Технические меры защиты информации реализуются в школе посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

5. Условия работы с информацией без использования средств автоматизации

5.1. Конфиденциальная информация, обрабатываемая в школе без использования средств автоматизации, должна обособляться от иной информации, в частности, путем фиксации на отдельных материальных носителях (далее - материальные носители), в специальных разделах или на полях форм (бланков). При этом, не допускается фиксация на одном материальном носителе различной информации, цели обработки которой заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

5.2. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию школы или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом школы, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации лицами, допуск которых к конфиденциальной информации не разрешён соответствующим приказом, не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию школы.

5.3. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных,

подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части информации уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование информации, подлежащей уничтожению или блокированию.

5.4. Уничтожение информации или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую обработку такой информации.

5.5. Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

5.6. При работе с информацией без использования средств автоматизации уточнение сведений, содержащихся в такой информации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых изменениях либо путем изготовления нового материального носителя с уточненной информацией.

5.7. Меры по обеспечению безопасности при обработке информации, осуществляемой без использования средств автоматизации, сводятся к следующему:

- Обработка конфиденциальной информации должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
- Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
- При хранении материальных носителей должны соблюдаться условия, исключающие несанкционированный к ним доступ, в том числе:

  - персональные данные сотрудников и учащихся, находящиеся в работе, хранятся в специальных сейфах, препятствующих свободному доступу лиц, не имеющих допуска к такой информации и материальным носителям,

  - архивные документы (материальные носители, выбывшие из оборота ввиду истечения определённого срока) хранятся с специально отведённом для этих целей помещении, ответственность за которое несет сотрудник, назначенный приказом директора,

  - педагоги, использующие в работе материальные носители с конфиденциальной информацией (персональными данными учащихся, их родителей (законных представителей)), несут персональную ответственность за сохранность и недоступность таких материальных носителей, определяя места хранения таких

носителей самостоятельно, с учётом безусловного соблюдения требований о недопущении несанкционированного доступа третьих лиц.

6. Использование сети «Интернет»

6.1. К объектам информационной безопасности в Школе при использовании сети «Интернет» относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- персональные данные;
- средства и системы информатизации – средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации;
- входящая и исходящая электронная переписка и документация.

6.2. Система информационной безопасности школы 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);
- установление чёткого перечня работников школы, допущенных к электронной почте школы, а также определение должностного лица, ответственного за надлежащее использование электронных почтовых ящиков учреждения и уничтожение переписки в электронных почтовых ящиках;
- установление единого порядка движения электронных документов с момента их создания (поступления) до отправки (передачи на хранение), основанного на следующих принципах:
  - централизация операций по приему электронных документов;
  - организация предварительного рассмотрения поступающих электронных документов;
  - однократность регистрации электронных документов;
  - согласование проектов электронных документов.

6.3. В сети «Интернет» школа размещает информацию, к которой должна быть в силу закона обеспечена свобода доступа, а также оказывает электронные услуги.

6.3.1. При размещении в сети «Интернет» информации, доступ к которой свободен для третьих лиц, а также при использовании электронного почтового ящика школы сотрудники школы должны соблюдать следующие условия:

- полный запрет на размещение конфиденциальной информации, правообладатель которой не дал своего письменного согласия на распространение информации в сети «Интернет»,
- персональные данные, без которых невозможно размещение носителя информации (приказы, локальные акты школы, статьи, публикации, и т.д.) в сети «Интернет» либо подлежат пересылке посредством электронного почтового ящика, должны быть максимально обезличены,
- персональные данные, подлежащие пересылке во исполнение официальных запросов властных полномочных органов и организаций, участвующих в обороте

персональных данных, подлежат пересылке в закодированном виде либо по защищённым каналам, доступ к которым устанавливается отдельным приказом директора.

6.3.2. Школа оказывает следующие электронные услуги:

- прием заявлений;
- предоставление информации об образовательных программах;
- предоставление информации о текущей успеваемости обучающихся;
- ведение электронного журнала успеваемости и электронного дневника;
- предоставление информации о порядке проведения государственной (итоговой) аттестации обучающихся, освоивших образовательные программы основного общего и среднего (полного) общего образования;
- предоставление информации о результатах единого государственного экзамена.

6.3.3. Электронный документооборот в школе включает в себя:

- формирование электронных документов;
- отправку и получение электронных документов;
- проверку электронных документов;
- учёт электронных документов;
- хранение электронных документов.

6.4. Организация и систематический контроль за электронным документооборотом в школе распределяется между ответственными сотрудниками в пределах их полномочий и должностных обязанностей приказом директора школы.

6.5. Использование сети «Интернет» в школе в целях организации образовательного процесса осуществляется с соблюдением следующих условий:

- применение учащимися интернет-ресурса осуществляется под строгим и непрерывным контролем со стороны педагогического персонала,
- доступ к компьютерам с выходами в сеть «Интернет» для учащихся попускается под присмотром учителя, педагога,
- помещения с компьютерами, имеющими выход в сеть «Интернет» в отсутствие сотрудников должны быть закрыты во избежание несанкционированного доступа со стороны учащихся,
- на компьютерах, которые доступны для учащихся и сотрудников школы, устанавливается контент-фильтрация,
- в рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности и по иным образовательным направлениям заинтересованное лицо может осуществлять доступ к ресурсам вне контент-фильтра, при соблюдении установленных законом дополнительных требований безопасности,
- работникам школы разрешено размещать в сети «Интернет» на интернет-ресурсах школы только информацию, относящуюся непосредственно к образовательной деятельности школы,
- работники школы вправе иметь личную учетную запись на интернет-ресурсах школы, данные о которой запрещено передавать третьим лицам,
- работники школы несут персональную ответственность за сохранность и конфиденциальность пароля доступа к автоматизированной информационной системе «Сетевой город. Образование»,

- работники школы обязаны раз в 3(три) месяца проводить смену личного пароля доступа к автоматизированной информационной системе «Сетевой город. Образование»,
- работникам запрещено размещать в сети «Интернет» и на интернет - ресурсах школы информацию не соответствующую требованиям законодательства РФ и локальным нормативным актам школы нарушающую нравственные и этические нормы, требования профессиональной этики.

6.6. При обнаружении в процессе работы ресурса, содержимое которого не совместимо с целями образовательной деятельности, он обязан незамедлительно сообщить об этом директору или ответственному за информационную безопасность школы с указанием интернет-адреса (URL) и покинуть данный ресурс.

6.7. Сотрудник школы, уполномоченный на обеспечение безопасности интернет-ресурса, обязан принять меры по отключению выхода на данный ресурс с интернет- ресурсов школы и сообщить о нём по специальной «горячей линии» для принятия мер в соответствии с законодательством РФ (в течение суток),если обнаруженный ресурс явно нарушает законодательство РФ. При этом, передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательной деятельности;
- дату и время обнаружения;
- информацию об установленных в школе технических средствах ограничения доступа к информации.

7. О системном администрировании и обязанностях ответственного за информационную безопасность

7.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы ответственного за информатизацию в школе.

7.2. Для решения задач информационной безопасности ответственный за информатизацию обязан:

- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);
- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
- обеспечивать нормальное функционирование системы резервного копирования.

8. Антивирусная защита

8.1. На компьютерах, используемых учащимися в учебной деятельности, устанавливается программное обеспечение, блокирующее доступ к негативной информации, которое обеспечено провайдером и программной поддержкой

браузера (фильтр-контент);

8.2. Учащимся закрыт доступ к сети «Интернет» через Wi-fi в местах общего пользования школы (библиотеки, коридоры и учебные кабинеты) с помощью пароля и прокси-сервера;

8.3. Исключена возможности установки на школьные компьютеры игр и другого программного продукта, не связанных с образовательным процессом.

8.4. Мониторинг качества работы системы контентной фильтрации в школе проводится ежедневно.

9. Заключительные положения

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

9.2. Сотрудники, работающие с информацией, ограниченной в обороте, несут дисциплинарную, административную и уголовную ответственность за требований законодательства по обеспечению информационной безопасности.