муниципальное бюджетное общеобразовательное учреждение
«Балезинская средняя общеобразовательная школа № 3»
(МБОУ «Балезинская средняя школа № 3»)

Согласовано
Советом школы
Протокол № 11 от 28.03. 2022 г

Утверждаю
Директор И.А.Жуйкова
Введено в действие приказом № 79-ОД
от 04 апреля 2022 года

ПОЛОЖЕНИЕ
о защите информации
в МБОУ «Балезинская средняя школа № 3»

I. Общие положения.

1.1. Настоящее Положение разработано в разработано в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ (ред. от 02.12.2019) «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ (ред. от 31.12.2017) «О персональных данных», Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Положение регулирует политику Школы по безопасности информационных и коммуникационных ресурсов и технологий и общий порядок обращения с документами, содержащими служебную информацию ограниченного распространения и устанавливает:

- объекты защиты информации и субъекты доступа к информации информационных систем и ресурсов;
- основные угрозы информационной безопасности;
- основные принципы построения системы защиты информации;
- меры, методы и средства обеспечения информационной безопасности.

1.3. Настоящее Положение разработано с целью установления надлежащего порядка и создания безопасных условий работы обучающихся и сотрудников Школы в информационных сетях.

II. Объекты и субъекты информационной безопасности

2.1. В Школе обрабатывается информация, содержащая сведения ограниченного распространения (служебная информация, персональные данные), и открытые сведения. Защите подлежат все информационные системы Школы, независимо от их местонахождения:

- информационные системы персональных данных, а также открытая (общедоступная) информация, необходимая для функционирования Школы, независимо от формы и вида ее предоставления;
- процессы обработки информации в информационных системах Школы, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

2.3. Особенности объектов информационной безопасности :

- объединение в единую систему большого количества технических средств обработки и передачи информации;
- необходимость непрерывности информационного обеспечения функционирования Школы;
- высокая интенсивность информационных потоков;

2.4. Особенности субъектов информационной безопасности:

2.4.1. разнообразие категорий пользователей:

- работники Школы (педагогический и технический персонал), участвующие в информационном обмене в соответствии с возложенными на них должностными обязанностями;
- обучающиеся Школы, осваивающие образовательные программы с применением информационных технологий;
- физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах Школы (в соответствии со ст.14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- сотрудники внешних организаций, занимающихся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем.

2.4.2. разный уровень знаний об информационных системах;

2.4.3. разный уровень и объем практического опыта работы в информационных системах;

2.4.4. разный уровень потребности в информационных системах.

2.5. Единство требований субъектов для доступа к информационным системам Школы:

- обеспечение своевременности доступа к необходимой информации;
- обеспечение достоверности, полноты, точности, целостности и актуальности информации;
- обеспечение конфиденциальности (сохранения в тайне) информации;
- защита от ложной (недостоверной, искаженной) информации;
- защита информации от незаконного распространения;
- предоставление возможности контроля и управления процессами обработки и передачи информации.

III. Цели и задачи системы обеспечения информационной безопасности.

3.1. Целью защиты информации, на достижение которой направлено настоящее Положение, является защита от возможного нанесения субъектом доступа к информации материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для авторизованных субъектов доступа (устойчивого функционирования системы, при котором авторизованные субъекты доступа имеют возможность получения необходимой информации);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационных системах Школы;
- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи. Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается методами и средствами, соответствующими множеству значимых угроз.

3.2. Для достижения основной цели защиты и обеспечения указанных свойств информации система информационной безопасности должна обеспечивать решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем;
- создание механизма оперативного реагирования на угрозы безопасности информации;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационных систем Школы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам - обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных (ученических) обязанностей;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в системах программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.3. Основные пути решения задач системы информационной безопасности Школы:
- учёт всех подлежащих защите информационных систем;
- учёт действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнота, реальная выполнимость и непротиворечивость требований локальных нормативных актов Школы по вопросам обеспечения информационной безопасности;
- подготовка должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности;
- наделение каждого работника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам;
- четкое знание и строгое соблюдение всеми пользователями информационных систем Школы, требований ее локальных нормативных актов по вопросам обеспечения информационной безопасности;
- персональная ответственность за свои действия каждого работника (обучающегося, родителя, законного представителя обучающегося), в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам;
- непрерывность поддержания необходимого уровня защищенности элементов информационных систем;
- применение программно-аппаратных средств защиты информации и непрерывной административной поддержкой их использования;
- эффективный контроль над соблюдением пользователями информационных ресурсов требований по обеспечению информационной безопасности.

IV. Основные угрозы и источники информационной безопасности Школы

4.1. Существует два вида угроз информационной безопасности:
- искусственные – угрозы, вызванные деятельностью человека;
- естественные – угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов техногенного характера или стихийных природных явлений, не зависящих от человека.

4.2. Наиболее значимыми угрозами информационной безопасности Школы (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение функциональности компонентов информационных систем, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных ресурсов, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) персональных данных.

.

4.3. Основные источники искусственных угроз информационной безопасности:

4.3.1. Непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации, приводящие к разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем:

- неосторожные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем;
- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (ключей (логинов), паролей, ключевых носителей и т. п.);
- игнорирование установленных правил при работе с информационными ресурсами;
- проектирование алгоритмов обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационных систем и информационной безопасности;
- пересылка информации по ошибочному электронному адресу (устройства); ввод ошибочных данных;
- неосторожная порча носителей информации;
- неосторожное повреждение каналов связи;
- неправомерное отключение оборудования или изменение режимов работы элементов информационных систем;
- заражение компьютеров вирусами;
- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности элементов информационных систем или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных);
- некомпетентное использование, настройка или неправомерное отключение средств защиты

4.3.2. Преднамеренные (в корыстных целях, по принуждению третьих лиц, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам пользователей, которые приводят к разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности элементов информационных систем:

- умышленные действия, приводящие к частичному или полному нарушению функциональности элементов информационных систем;
- действия по дезорганизации функционирования информационных систем, хищение электронных документов и носителей информации; несанкционированное копирование электронных документов и носителей информации;
- умышленное искажение информации, ввод неверных данных;

- отключение или вывод из строя подсистем обеспечения функционирования элементов информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи);
- перехват данных, передаваемых по каналам связи и их анализ;
- незаконное получение атрибутов разграничения доступа (используя халатность пользователей, путем подделки, подбора пароля);
- несанкционированный доступ к ресурсам информационных систем с рабочих станций авторизованных субъектов доступа;
- хищение или вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования элементов информационных систем Учреждения;
- незаконное использование элементов информационных систем, нарушающее права третьих лиц;
- применение подслушивающих устройств, фото и видео съемка для несанкционированного съема информации.

4.3.3. Удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (прежде всего через сеть Интернет), через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к информационным ресурсам;

- ошибки, допущенные при разработке элементов информационных систем и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации);
- технические сбои элементов информационных систем.

4..4. Основные естественные угрозы информационной безопасности:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;
- выход из строя или невозможность использования линий связи;
- пожары и другие стихийные бедствия.

V. Основные принципы построения системы защиты информации

5.1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы защиты информации в соответствии с действующим законодательством в области информации, информатизации и защиты информации.

5.2. Системность.

Предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность.

Предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз.

5.4. Непрерывность защиты.

Предполагает постоянную организационную (административную) поддержку (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий).

5.5. Своевременность.

Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем.

5.6. Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и систем информационной защиты.

5.7. Персональная ответственность.

Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника в пределах его полномочий.

5.8. Минимизация полномочий.

Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью.

5.9. Гибкость системы информационной безопасности.

Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления Школой своей деятельности.

5.10. Простота применения средств защиты.

Механизмы и методы системы защиты информации должны быть понятны и просты в использовании.

5.11. Обоснованность и техническая реализуемость.

Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

5.12. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.

5.13. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей..

VI. Меры, методы и средства обеспечения информационной безопасности.

6.1. Меры обеспечения информационной безопасности.

6.1.1. Законодательные (правовые) меры.

К ним относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем Учреждения.

6.1.2. Технологические меры.

К ним относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.1.3. Организационные (административные) меры.

Это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой. Такими мерами являются:

- регламентация доступа в здание Школы;
- регламентация допуска работников к использованию информационных ресурсов;
- анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;
- обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники;
- обучение пользователей;
- деятельность по обеспечению информационной безопасности;
- условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами Учреждения.

6.1.4. Физические меры..

Основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

6.1.5. Технические (аппаратно-программные) меры.

Основаны на использовании электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

VII. Особенности обработки информации, содержащей персональные данные.

7.1. Все персональные данные субъекта Школы следует получать у него самого (для обучающихся - от родителей (законных представителей). Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

Должностное лицо Школы должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению ПД и последствиях отказа дать письменное согласие на их получение.

7.2. Учреждение не имеет права получать и обрабатывать данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях,

непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

7.3. Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку.

7.4. Обработка указанных данных возможна без его согласия в соответствии со ст.6 Федеральным законом от 27.07.2006 №152 «О персональных данных».

7.5. Согласие на обработку персональных данных оформляется в письменном виде.

7.6. Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных; цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных
- срок, в течение которого действует согласие, а также порядок его отзыва.

7.7. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу на имя директора Школы.

7.8. Субъект персональных данных имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7.9. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

7.10. Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться в персональных данных, относящиеся к другим субъектам персональных данных.

7.11. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя. Письменный запрос должен быть адресован на имя директора Школы или уполномоченного руководителем лицо.

7.12. Субъект в праве обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия персональных данных должностных лиц Школы при обработке и защите его персональных данных.

VIII. Обязанности и права должностных лиц.

8.1. Директор Школы организует работу по построению системы защиты информационной системы. В частности:

- назначает ответственного за организацию защиты информации из числа сотрудников Школы;
- утверждает круг лиц, имеющих доступ к защищаемой информации и порядок их работы;
- утверждает комплект документов, определяющих политику в отношении защиты информации в учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ.

8.2. Ответственный за защиту информации:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью информационной системы;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- обеспечивает защиту информации, циркулирующей на объектах информатизации;
- проводит систематический контроль работы систем защиты информации, применяемых в информационной системе, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей информационной системы;
- контролирует выполнение администратором информационной системы обязанностей по обеспечению функционирования систем защиты информации (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам информационной системы, антивирусная защита, резервное копирование данных и т.д.);
- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;
- участвует в работах по внесению изменений в аппаратно-программную конфигурацию информационной системы;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав информационной системы;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к информационной системе;
- требует устранения выявленных нарушений и недостатков, дает обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения, незамедлительно принимает меры пресечения и докладывает руководителю Учреждения;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

8.3. Несоответствие мер установленным требованиям или нормам по защите информации, является нарушением и влечёт административное наказание ответственных лиц в соответствии с законодательством РФ.

IX. Заключительные положения.

9.1. Положение вступает в силу с момента его утверждения.

9.2. Положение является локальным актом Школы. Внесение изменений и дополнений в Положение осуществляется в порядке его принятия.