Муниципальное автономное общеобразовательное учреждение
«Лицей №7»

Утверждаю
И.о. директора МАОУ «Лицей №7»
_____ Мещерякова Е.В.
Приказ № 371
от «28» октября 2026 г.

Политика защиты информации
в Муниципальном автономном общеобразовательном учреждении
«Лицей №7» города Бердска

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Назначение и область действия документа.

Настоящая Политика защиты информации (далее – Политика) определяет цели, задачи, принципы, организационную структуру и основные направления деятельности по защите информации, обрабатываемой в информационных системах (далее – ИС) Муниципального автономного общеобразовательного учреждения «Лицей №7» (далее – МАОУ «Лицей №7»).

Политика устанавливает единые подходы к формированию, функционированию и развитию системы защиты информации, а также является обязательной для применения при разработке иных локальных нормативных актов, регламентирующих вопросы информационной безопасности.

Требования Политики также обязательны для подрядных организаций и иных третьих лиц, привлекаемых к выполнению работ или оказанию услуг, связанных с доступом к ИС МАОУ «Лицей №7» либо к информации, обрабатываемой в них. Соблюдение указанных требований обеспечивается посредством включения соответствующих обязательств в договорную документацию и контроля их исполнения.

Действие настоящей Политики распространяется на:

всех сотрудников МАОУ «Лицей №7» независимо от занимаемой должности и характера выполняемых обязанностей, в части, касающейся их участия в обработке информации и эксплуатации ИС;

все ИС МАОУ «Лицей №7», а также связанные с ними сегменты сети, площадки размещения, программно-аппаратные средства и элементы информационно-телекоммуникационной инфраструктуры, перечень которых утверждается приказом директора МАОУ «Лицей №7».

2. Нормативно-правовые акты, методические документы, национальные стандарты.

Политика разработана в соответствии с:

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 персональных данных»;

Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Указом Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

Приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

Методическим документом ФСТЭК России 2026 г. «Мероприятия и меры по защите информации, содержащейся в информационных системах»;

Трудовым кодексом Российской Федерации (в части регулирования обязанностей сотрудников по соблюдению требований защиты информации);

национальными стандартами Российской Федерации в области защиты информации и информационной безопасности;

иными нормативными и методическими документами ФСТЭК России, ФСБ России.

3. Термины и определения.

Термины и определения, используемые в настоящей Политике, применяются в значениях, установленных нормативными правовыми актами Российской Федерации и нормативными документами, указанными в пункте I.2 настоящего документа.

При отсутствии специальных определений в указанных нормативных правовых актах используются термины и определения, закрепленные в национальных стандартах Российской Федерации, в том числе:

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

ГОСТ Р 56545-2015 «Защита информации. Информация и информационные технологии. Термины и определения»;

ГОСТ Р 56546-2015 «Защита информации. Обеспечение информационной безопасности. Термины и определения».

В случае расхождения формулировок приоритет имеют определения, установленные федеральными законами и иными нормативными правовыми актами Российской Федерации.

Использование терминов в настоящей Политике осуществляется в целях обеспечения единообразного понимания требований по защите информации и недопущения неоднозначного толкования положений документа.

II. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

1. Целью обеспечения защиты информации в МАОУ «Лицей №7» является поддержание установленного уровня конфиденциальности, целостности и доступности информации, обрабатываемой в ИС, а также обеспечение устойчивости и непрерывности их функционирования посредством предупреждения и нейтрализации актуальных угроз безопасности информации и недопущения наступления неприемлемых последствий (ущерба) для деятельности МАОУ «Лицей №7».

2. Для достижения поставленной цели защиты информации МАОУ «Лицей №7» решает следующие задачи:

1) определение недопустимых событий, связанных с нарушением безопасности информации;

2) систематическое выявление и оценка угроз безопасности информации;

3) реализация организационных и технических мер защиты информации, адекватных актуальным угрозам и классу защищённости ИС;

4) управление конфигурациями ИС и их уязвимостями;

5) непрерывный мониторинг информационной безопасности и реагирование на инциденты;

6) обеспечение физической защиты компонентов ИС;

7) поддержание необходимого уровня знаний пользователей по вопросам защиты информации.

III. ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Деятельность по обеспечению защиты информации в МАОУ «Лицей №7» осуществляется на основе следующих принципов:

Законность – соблюдение требований законодательства Российской Федерации, нормативных правовых актов уполномоченных органов и локальных нормативных актов Организации при организации и реализации мер защиты информации.

Непрерывность – обеспечение защиты информации на всех этапах жизненного цикла ИС (проектирование, создание, ввод в эксплуатацию, эксплуатация, модернизация и вывод из эксплуатации), а также во всех режимах их функционирования.

Адекватность – соответствие применяемых мер защиты характеру актуальных угроз безопасности информации, категории и уровню защищенности ИС, а также потенциальным возможностям нарушителя.

Минимизация прав и привилегий – предоставление субъектам доступа исключительно тех прав и полномочий, которые необходимы для выполнения возложенных на них функций (принцип минимально необходимых прав, «необходимо знать»).

Многоуровневость (эшелонированность) – построение системы защиты информации по принципу последовательных и взаимодополняющих уровней защиты с использованием различных по типу и назначению средств и механизмов.

Персональная ответственность – закрепление обязанностей по обеспечению защиты информации за конкретными работниками в соответствии с их должностными обязанностями и локальными нормативными актами Организации.

Управляемость и контролируемость – обеспечение возможности планирования, мониторинга и оценки эффективности реализуемых мер защиты информации, а также своевременного выявления и устранения выявленных недостатков.

IV. ОБЪЕКТЫ ЗАЩИТЫ

Защите подлежат:

1) информационные ресурсы (информация ограниченного доступа, включая персональные данные, служебную информацию и т.д.), обрабатываемые в ИС;

2) программные, программно-аппаратные и технические средства, входящие в состав ИС (серверы, автоматизированные рабочие места, сетевое оборудование, средства хранения данных, средства защиты);

3) информационно-телекоммуникационная инфраструктура, на базе которой функционирует ИС (включая каналы связи, активное оборудование);

4) машинные носители информации (съёмные и стационарные);

5) помещения (контролируемая зона), где размещены компоненты ИС.

V. КАТЕГОРИИ ЛИЦ, УЧАСТВУЮЩИХ В ЗАЩИТЕ ИНФОРМАЦИИ, ИХ ОБЯЗАННОСТИ (ФУНКЦИИ) И ПОЛНОМОЧИЯ

1. Состав действующих лиц. Деятельность по защите информации в МАОУ «Лицей №7» осуществляется с участием следующих категорий лиц:

директор МАОУ «Лицей №7»;

ответственный за организацию защиты информации;

ответственный за техническую защиту информации;

ответственный за выполнение требований законодательства при эксплуатации средств криптографической защиты информации (далее - СКЗИ);

ответственный за организацию обработки персональных данных (далее - ПДн);

ответственный за обеспечение безопасности ПДн;

пользователи ИС (сотрудники МАОУ «Лицей №7», внешние пользователи).

2. Распределение обязанностей и полномочий между указанными лицами закрепляется настоящей Политикой, а также приказами МАОУ «Лицей №7», должностными инструкциями и иными внутренними локальными актами МАОУ «Лицей №7».

3. **Директор МАОУ «Лицей №7».**

Основные обязанности (функции): утверждает Политику защиты информации и иные локальные акты; назначает ответственных лиц в области защиты информации; определяет структуру управления; осуществляет ресурсное обеспечение мероприятий по защите информации; осуществляет общий контроль за состоянием защищенности; принимает решения по результатам расследований серьезных инцидентов информационной безопасности; обеспечивает

взаимодействие с уполномоченными государственными органами по вопросам защиты информации.

Права: назначать ответственных лиц и допускать пользователей; утверждать внутренние локальные акты по защите информации; распределять бюджетные средства на мероприятия по защите информации; инициировать служебные проверки и применять дисциплинарные взыскания.

4. **Ответственный за организацию защиты информации.**

Основные обязанности (функции): организует выполнение организационных и технических мер защиты; контролирует соблюдение нормативно-правовых актов; координирует деятельность сотрудников по защите информации; организует проведение оценки состояния защиты; организует обучение сотрудников; планирует мероприятия по повышению уровня защищенности; взаимодействует с подрядными организациями по вопросам защиты информации; докладывает руководителю о состоянии защищенности, а также о необходимости дополнительных ресурсов.

Права: запрашивать у структурных подразделений информацию, необходимую для выполнения задач; давать обязательные для исполнения указания в пределах своей компетенции; инициировать служебные расследования инцидентов; приостанавливать работу ИС при выявлении критических угроз (с незамедлительным уведомлением руководителя); представлять МАОУ «Лицей №7» в вопросах защиты информации перед третьими лицами; вносить предложения о совершенствовании системы защиты информации.

5. **Ответственный за техническую защиту информации.**

Основные обязанности (функции): реализует организационные и технические меры защиты информации в закрепленных за ним ИС; разрабатывает и актуализирует локальные акты по защите информации в ИС; управляет учетными записями в соответствии с установленными правилами; настраивает и эксплуатирует средства защиты информации; осуществляет управление уязвимостями (выявление, устранение (нейтрализация)); контролирует конфигурации ИС, выявляет и устраняет уязвимости, управляет обновлениями программного обеспечения; осуществляет мониторинг событий безопасности, выявляет инциденты и принимает меры по реагированию; контролирует процедуры резервного копирования; выполняет оценку показателей защищенности; уведомляет о выявленных инцидентах ответственного за организацию защиты информации.

Права: проводить настройку средств защиты информации; блокировать доступ пользователей при нарушении требований безопасности; требовать от пользователей соблюдения правил работы в ИС; инициировать внеочередные проверки защищенности; запрашивать у подразделений, обеспечивающих техническое обслуживание, информацию, необходимую для выполнения обязанностей; вносить предложения о совершенствовании системы защиты информации.

6. **Ответственный за выполнение требований законодательства при эксплуатации СКЗИ.**

Основные обязанности (функции): разрабатывает и актуализирует локальные акты по защите информации с применением СКЗИ; настраивает СКЗИ в соответствии с требованиями по эксплуатации; осуществляет ведение журналов

учета СКЗИ; проводит инструктаж пользователей СКЗИ; контролирует условия эксплуатации СКЗИ; подготавливает заключения о возможности допуска пользователей к самостоятельной работе с СКЗИ, а также о возможности эксплуатации СКЗИ; информирует о нарушениях ответственного за организацию защиты информации, а также в случае серьезных нарушений директору МАОУ «Лицей №7».

Права: осуществлять учет и контроль использования криптографических средств; отказывать в допуске к работе с СКЗИ при несоответствии требованиям (с незамедлительным уведомлением ответственного за организацию защиты информации); инициировать замену или обновление криптографических средств; требовать соблюдения правил хранения ключевой информации; приостанавливать эксплуатацию СКЗИ при нарушении условий их применения.

7. **Ответственный за организацию обработки Пдн.**

Основные обязанности (функции): разрабатывает и актуализирует локальные акты по защите ПДн; контролирует законность обработки ПДн, в том числе наличия согласий; работает с обращениями субъектов ПДн; обеспечивает конфиденциальность бумажных и электронных носителей, содержащих ПДн; информирует о нарушениях директору МАОУ «Лицей №7».

Права: получать доступ к ИС, базам данных и документам, содержащим персональные данные, в объеме, необходимом для выполнения контрольных функций; требовать от подразделений соблюдения правил обработки ПДн; инициировать служебные проверки по фактам нарушений; представлять МАОУ «Лицей №7» во взаимодействии с Роскомнадзором (при необходимости); вносить предложения о совершенствовании системы защиты ПДн.

8. **Ответственный за обеспечение безопасности Пдн.**

Основные обязанности (функции): проводит инвентаризацию активов с ПДН; выполняет установку и настройку оборудования и программных средств в ИСПДн; осуществляет обслуживание сетевого оборудования, серверов и автоматизированных рабочих станций в ИСПДн; контролирует целостность программно-аппаратной среды в ИСПДн; устраняет технические неисправности и ошибки в работе программного обеспечения в ИСПДн; информирует о нарушениях ответственного за организацию обработки ПДн.

Права: получать доступ к оборудованию и системному программному обеспечению в ИПСДн; изменять конфигурации технических средств в рамках утвержденных процедур в ИСПДн; приостанавливать эксплуатацию оборудования при выявлении угроз безопасности ПДн (с незамедлительным уведомлением ответственного за организацию обработки ПДн); запрашивать у структурных подразделений и пользователей информацию, необходимую для технического обслуживания и устранения неисправностей в ИСПДн.

9. **Пользователи ИС.**

Основные обязанности (функции): соблюдать требования настоящей Политики, регламентов и инструкций при работе в ИС; использовать ИС исключительно для выполнения служебных задач; сохранять конфиденциальность учетных данных (паролей, токенов) и не передавать их третьим лицам; незамедлительно уведомлять ответственного за организацию защиты информации

или ответственного за техническую защиту информации о подозрительных событиях, попытках несанкционированного доступа, утрате носителей информации или компрометации учетных записей; проходить инструктажи и обучение по вопросам информационной безопасности; не устанавливать несанкционированное программное обеспечение, не изменять настройки средств защиты информации.

Права: получать доступ к ИС, ресурсам и данным в объеме, необходимом для выполнения должностных обязанностей; использовать предоставленные программные и технические средства в соответствии с их назначением; запрашивать и получать информацию о действующих правилах обработки информации и политиках безопасности (в части, их касающейся); подавать заявки на предоставление, изменение или продление прав доступа к информационным ресурсам в установленном порядке; сообщать руководству и ответственным лицам о выявленных нарушениях, уязвимостях, инцидентах и подозрительной активности.

VI. ОРГАНИЗАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. Организационная структура.

В МАОУ «Лицей №7» применяется централизованная модель управления деятельностью по защите информации, при которой стратегическое руководство осуществляется директором МАОУ «Лицей №7», а оперативная реализация мероприятий распределяется между назначенными ответственными лицами.

Система управления деятельностью по защите информации функционирует на основе процессного подхода и принципов, изложенных в настоящей Политике, и охватывает все этапы жизненного цикла ИС.

2. Структура управления деятельностью по защите информации включает:

1) стратегический уровень – директор МАОУ «Лицей №7»;

2) координационный уровень – ответственный за организацию защиты информации;

3) функциональный уровень – ответственный за техническую защиту информации, ответственный за выполнение требований законодательства при эксплуатации СКЗИ, ответственный за организацию обработки Пдн, ответственный за обеспечение безопасности Пдн;

4) исполнительный уровень – пользователи ИС.

3. Механизмы взаимодействия и контроля:

1) вертикальные связи – в порядке подчиненности и отчетности:

ответственный за организацию защиты информации отчитывается перед директором МАОУ «Лицей №7»;

функциональные специалисты отчитываются перед ответственным за организацию защиты информации;

пользователи информируют ответственных лиц о подозрительных событиях.

2) горизонтальные связи – между функциональными специалистами:

ответственный за обеспечение безопасности Пдн взаимодействуют с ответственным за организацию обработки Пдн;

ответственный за выполнение требований законодательства при эксплуатации СКЗИ взаимодействует с ответственным за техническую защиту информации.

3) условия совмещения ролей – в целях обеспечения рационального распределения кадровых ресурсов в МАОУ «Лицей №7» допускается возложение на одного сотрудника обязанностей по нескольким направлениям деятельности в области защиты информации. Совмещение ролей допускается исключительно при невозможности их разделения и при условии реализации компенсирующих мер, включая:

участие директора МАОУ «Лицей №7» в оценке эффективности защиты;

оценка состояния защиты должна проводиться с привлечением постоянно действующей комиссии;

сотрудник должен иметь необходимую квалификацию;

при необходимости допускается привлечение лицензиата ФСТЭК России.

4) коллегиальные органы – для решения общих вопросов и обеспечения независимой оценки директора МАОУ «Лицей №7» создаются:

комиссия по классификации информационных систем;

комиссия по уничтожению Пдн;

комиссия по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;

комиссия по осуществлению внутреннего контроля соответствия обработки ПДн.

5) формы контроля:

а) мониторинг информационной безопасности – осуществляется непрерывно;

б) периодический контроль уровня защищенности – осуществляется **коллегиальными органами** в установленные локальными актами сроки;

в) внутренние проверки (аудиты)- осуществляются планово, в соответствии с планами на отчетный период, и внепланово, в случае выявления нарушений по информационной безопасности или по решению директора МАОУ «Лицей №7»;

г) внешний аудит с привлечением лицензиата ФСТЭК России - осуществляется при необходимости по решению директора МАОУ «Лицей №7».

4. Условия привлечения лицензиата. В целях обеспечения независимой оценки состояния защиты информации МАОУ «Лицей №7» вправе привлекать юридическое лицо, имеющее лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации. Привлечение лицензиата рекомендуется при:

отсутствии в штате независимого компетентного специалиста по защите информации;

подготовке к аттестации ИС;

существенных изменениях архитектуры ИС;

выявлении инцидентов информационной безопасности;

необходимости проведения независимой оценки эффективности системы защиты информации.

VII. МЕРОПРИЯТИЯ (ПРОЦЕССЫ) ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. Обеспечение защиты информации в МАОУ «Лицей №7» осуществляется на основе системного подхода и достигается не разовым применением отдельных технических или организационных средств, а посредством непрерывной реализации комплекса взаимосвязанных мероприятий (процессов), охватывающих все этапы жизненного цикла ИС – от их проектирования и ввода в эксплуатацию до модернизации и вывода из эксплуатации.

2. Эффективность защиты информации зависит от полноты внедрения установленных процессов, уровня компетенции работников, участвующих в их реализации, а также от актуальности и достаточности организационно-распорядительной и эксплуатационной документации.

3. Каждый процесс защиты информации подлежит регламентации внутренними нормативными документами МАОУ «Лицей №7», определяющими:

цели и задачи процесса;

порядок выполнения мероприятий;

сроки и периодичность их осуществления;

формы документирования и контроля.

VIII. МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. В МАОУ «Лицей №7» применяются организационные и технические меры защиты информации, обеспечивающие установленный уровень защищенности и исключающие возможность совершения в отношении информации неправомерных действий, включая несанкционированный доступ, изменение, уничтожение, блокирование, копирование или распространение.

2. Для ИС состав и объём реализуемых мер защиты информации определяется с учетом:

1) результатов классификации;

2) характера обрабатываемой информации;

3) актуальных угроз безопасности информации;

4) особенностей архитектуры;

5) требований нормативных правовых актов Российской Федерации.

3. В МАОУ «Лицей №7» функционирует система организационных мер защиты информации, обеспечивающая планирование, координацию, контроль и совершенствование деятельности в области информационной безопасности. Организационные меры направлены на создание управляемой системы защиты информации, в рамках которой определены структура управления, распределены обязанности и установлена персональная ответственность должностных лиц.

В целях реализации организационных мер:

действует утвержденная структура управления защитой информации, включающая назначенных ответственных лиц;

применяются локальные акты, регламентирующие обработку информации, порядок предоставления доступа, эксплуатацию ИС и средств защиты;

осуществляется предоставление, изменение и прекращение доступа сотрудников к информации и информационным ресурсам в установленном порядке;

проводится ознакомление сотрудников с требованиями по защите информации и обеспечивается подтверждение их обязательств по соблюдению установленных правил;

организуется регулярное обучение и инструктаж сотрудников по вопросам информационной безопасности;

осуществляется внутренний контроль соблюдения требований защиты информации, включая проведение проверок и анализ выявленных нарушений;

обеспечивается документирование процессов защиты информации и хранение соответствующей документации;

при привлечении подрядных организаций требования информационной безопасности закрепляются в договорных обязательствах и контролируются в ходе выполнения работ.

4. В ИС МАОУ «Лицей №7» применяется комплекс технических мер защиты информации, обеспечивающий установленный уровень защищенности и устойчивость функционирования информационной инфраструктуры. Технические меры реализуются с учетом оценки угроз, категории и уровня защищенности ИС, а также особенностей их архитектуры и эксплуатации.

В рамках реализации технических мер:

обеспечивается идентификация и аутентификация пользователей и администраторов, включая применение усиленных механизмов аутентификации для привилегированных учетных записей;

действует разграничение доступа к информационным ресурсам в соответствии с установленными ролями и принципом минимально необходимых прав;

осуществляется регистрация и анализ событий безопасности, обеспечивается защита журналов регистрации;

применяются средства антивирусной защиты, поддерживается актуальность их баз и программных компонентов;

функционируют средства межсетевого экранирования и сегментации сети, обеспечивается фильтрация сетевого трафика;

используются средства обнаружения вторжений и выявления аномальной активности;

осуществляется контроль целостности программных средств и конфигураций ИС;

выполняется резервное копирование информации, обеспечивается хранение резервных копий и возможность восстановления данных;

передача информации осуществляется с использованием защищённых протоколов и, при необходимости, СКЗИ;

ограничивается физический доступ к средствам обработки информации, применяются средства контроля и управления доступом на защищаемые территории;

обеспечивается устойчивость функционирования ИС, включая резервирование критически важных компонентов.

IX. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ

1. Сотрудники МАОУ «Лицей №7», а также иные лица, допущенные к обработке информации и эксплуатации ИС, несут ответственность за соблюдение требований законодательства Российской Федерации в области защиты информации, настоящей Политики и иных локальных актов МАОУ «Лицей №7».

2. Нарушение требований о защите информации влечёт ответственность в соответствии с трудовым законодательством Российской Федерации, гражданским, административным и уголовным законодательством Российской Федерации.

3. Привлечение к ответственности осуществляется независимо от занимаемой должности и уровня доступа к ИС. Ответственность может наступать как при наличии наступивших негативных последствий, так и при создании угрозы их возникновения.

4. Основанием для привлечения к ответственности является установление факта нарушения требований о защите информации, выразившегося в:

1) несоблюдении требований настоящей Политики;

2) нарушении порядка обработки информации ограниченного доступа;

3) разглашении конфиденциальной информации;

4) несанкционированном доступе к ИС;

5) передаче учетных данных третьим лицам;

6) несанкционированном изменении конфигураций;

7) несвоевременном уведомлении о выявленных инцидентах информационной безопасности;

8) нарушении требований эксплуатации средств защиты информации.

5. Ответственные лица в области защиты информации несут персональную ответственность за:

1) неисполнение или ненадлежащее исполнение возложенных обязанностей;

2) отсутствие должного контроля в пределах своей компетенции;

3) несвоевременное принятие мер по устранению выявленных нарушений;

4) непринятие мер реагирования при выявлении инцидентов информационной безопасности.

Совмещение обязанностей не освобождает должностное лицо от ответственности по каждому направлению деятельности.