УТВЕРЖДЕНО

приказ заместителя директора – главного инженера

УП «Брествторчермет»

От 02.06.2026 г №136

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УП «БРЕСТВТОРЧЕРМЕТ»

2026 г.

СОДЕРЖАНИЕ

1. Введение

Политика информационной безопасности (далее – Политика ИБ) УП «Брествторчермет» разработана в соответствии с требованиями Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66, и содержит описание реализации организационных и технических мер по защите информации в информационных системах УП «Брествторчермет».

2. Определения, обозначения и сокращения

2.1. В настоящем документе применяются термины и их обозначения установленные:

Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Законом Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

Положением о технической и криптографической защите информации, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196;

Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

2.2. Также в Политике ИБ применяются следующие термины и их обозначения:

информационная безопасность – состояние защищенности информационного пространства, информационной инфраструктуры и информационных ресурсов от внешних и внутренних угроз в информационной сфере;

отказ – событие, состоящее из нарушения работоспособности средств вычислительной техники, средств технической защиты информации и иных технических средств из состава информационной системы, для восстановления которой требуется замена составной части или регулировка (настройка);

пароль – набор знаков, предназначенный для подтверждения личности и (или) полномочий;

подлинность – свойство информации, гарантирующее, что информация идентична оригинальной (заявленной);

программное обеспечение – совокупность программных средств (изделий), данных и инструкций, предназначенных для выполнения задач на компьютерах и других электронных вычислительных устройствах;

сохранность – свойство информации, гарантирующее, что информация ни при каких условиях не может быть уничтожена (удалена);

средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности;

целостность – свойство сохранения точности и полноты (комплектности).

2.3. В Политике ИБ применяют следующие сокращения

ИБ – информационная безопасность;
ИС – информационная система;
ЛПА – локальный правовой акт;
ОРД – организационно-распорядительный документ;
СЗИ – система защиты информации;
ТКЗИ – техническая и криптографическая защита информации.

3. Общие положения

3.1. Политика ИБ – это официально сформулированные общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации при ее обработке в УП «Брествторчермет».

3.2. Политика ИБ документируется с учетом требований нормативных правовых актов Республики Беларусь, регламентирующих деятельность по защите информации.

3.3. Политика ИБ под роспись доводится до сведения работников УП «Брествторчермет», должна быть доступной всем заинтересованным субъектам информационных отношений для ознакомления.

3.4. Положения Политики ИБ распространяются на сторонние организации, взаимодействующие с УП «Брествторчермет».

3.5. Политика ИБ служит основой для проведения работ по защите информации и определяет пути совершенствования системы защиты информации (далее – СЗИ).

3.6. Руководство УП «Брествторчермет» обязуется соответствовать требованиям по защите информации и постоянно совершенствовать СЗИ.

3.7. Политика ИБ является методологической основой для:

проведения мероприятий в области обеспечения ИБ в УП «Брествторчермет» в рамках принятия управленческих решений, разработки и реализации комплекса согласованных мер, направленных на выявление различных видов угроз ИБ, противодействие им, а также ликвидацию последствий их проявления;

координации деятельности работников при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению ИБ;

разработки предложений по совершенствованию нормативного, технического и организационного обеспечения ИБ в УП «Брествторчермет»;

разработки локально-правовых актов (далее – ЛПА) и организационно-распорядительных документов (далее – ОРД), регламентирующих вопросы защиты информации в информационной системе (далее – ИС), предназначенных для обработки информации.

3.8. В целях защиты активов доступ к ним ограничивается, управляется и контролируется в соответствии с ЛПА и ОРД по вопросам применения СЗИ УП «Брествторчермет».

Предоставление доступа к активам УП «Брествторчермет» третьим лицам должно осуществляться на основании подписанного письменного соглашения о безусловном принятии положений настоящей Политики ИБ, а также, при необходимости, комплекта ЛПА, ОРД по вопросам применения СЗИ (выдержек из ЛПА, ОРД по вопросам применения СЗИ)

УП «Брествторчермет» в области защиты информации в зависимости от выполняемых работ.

В указанные соглашения также включаются определение, предоставление и условия доступа к активам, ответственность сторон.

3.9. Реализация Политики ИБ должна осуществляться на основе принципов непрерывности и строгого соблюдения установленных правил.

3.10. Руководство УП «Брествторчермет», а также ответственный за техническую и криптографическую защиту информации (далее – ответственный за ТКЗИ) проводят анализ Политики ИБ с целью обеспечения ее постоянной пригодности и эффективности.

3.11. Нарушение требований Политики ИБ влечет ответственность в соответствии с законодательством Республики Беларусь.

3.12. Контроль исполнения Политики ИБ выполняется уполномоченными должностными лицами, ответственными за обеспечение ИБ (защиты информации) в УП «Брествторчермет», в зависимости от объема возложенных в этой области на них обязанностей.

4. Цели и принципы защиты информации

4.1. Основными целями защиты информации являются:

установление в УП «Брествторчермет» подходов к обеспечению защиты информации, распространение и (или) предоставление которой ограничено;

недопущение неправомерного доступа, уничтожения, модификации, копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий;

сохранение и неразглашение в УП «Брествторчермет» информации, распространение и (или) предоставление которой ограничено;

сохранность и неразглашение информации, распространение и (или) предоставление которой ограничено, предоставляемой в соответствии с договорами (соглашениями) УП «Брествторчермет» с другими субъектами информационных отношений;

обеспечение прав субъектов информационных отношений при внедрении и эксплуатации ИС;

воспрепятствование неправомерному нарушению целостности, доступности, сохранности, подлинности и конфиденциальности информации распространение и (или) предоставление которой ограничено при ее обработке в ИС;

минимизация ущерба от реализации угроз ИБ в УП «Брествторчермет».

4.2. Основными принципами защиты информации являются:

принцип законности. Применение мер и средств обеспечения защиты информации в строгом соответствии с законодательством Республики Беларусь;

принцип осведомленности. Каждый работник (пользователь ИС) должен быть осведомлен о предоставленных ему правах, а также накладываемых на него ограничениях, обязанностях и ответственности. Все работники УП «Брествторчермет» обязаны знать требования защиты информации в объеме, соответствующем их текущим должностным обязанностям и доступу к активам УП «Брествторчермет», и руководствоваться ими в своей работе;

принцип системности. Учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для обеспечения защиты информации в УП «Брествторчермет»;

принцип непрерывности. Деятельность по обеспечению защиты информации является составной частью повседневной деятельности УП «Брествторчермет» и не должна прерываться, обеспечивая непрерывный контроль выполнения требований защиты информации;

принцип документированности. Все требования и меры защиты информации, а также результаты деятельности по обеспечению защиты информации должны быть документально зафиксированы;

принцип недопустимости перехода в открытое состояние. При любых обстоятельствах (в том числе нештатных) СЗИ должна либо полностью выполнять свои функции, либо блокировать доступ;

принцип минимизации привилегий. Работники должны иметь только те права доступа, которые необходимы им для выполнения служебных обязанностей;

принцип разделения обязанностей. Должно быть обеспечено распределение ролей и ответственности, при котором один работник не может нарушить критически важный для УП «Брествторчермет» процесс;

принцип многоуровневой защиты. За средствами инженерно-физической защиты должны следовать программно-технические средства. Должна обеспечиваться идентификация и аутентификация пользователей, управление доступом, своевременное выявление и оценка причин, условий и характера угроз ИБ и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ, протоколирование и аудит событий безопасности;

принцип простоты и управляемости информационной системы и системы защиты информации. ИС и СЗИ должны быть максимально прозрачны в управлении, а их документация – четко проработана;

принцип всеобщей поддержки мер безопасности. Реализация программ по осведомленности и обучению работников УП «Брествторчермет» о возможных факторах рисков ИБ и мерах противодействия, постоянное обучение;

принцип персональной ответственности. Ответственность за обеспечение безопасности информации и системы ее обработки должна быть возложена на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников должно строиться таким образом, чтобы в случае любого нарушения круг причастных к инцидентам был четко известен или сведен к минимуму. Наличие должностных лиц, ответственных за ИБ в УП «Брествторчермет», а также работников, осуществляющих практическую работу по обеспечению защиты информации, должно быть определено организационной структурой (штатным расписанием) УП «Брествторчермет», приказами или должностными инструкциями.

5. Общие требования по обеспечению защиты информации

5.1. Обеспечение защиты информации в УП «Брествторчермет» – целенаправленный непрерывный процесс выполнения соответствующих мероприятий на всех этапах жизненного цикла применяемых активов ИС и средств защиты информации.

5.2. Защите должна подвергаться вся информация, содержащаяся в ИС УП «Брествторчермет», неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю.

5.3. Требования по защите общедоступной информации устанавливаются в целях обеспечения доступности и целостности.

5.4. Общее руководство обеспечением защиты информации, координацию работ и контроль за исполнением мероприятий по ИБ осуществляет лицо, назначенное приказом.

5.5. Ответственный за ТКЗИ в УП «Брествторчермет» назначается приказом.

5.6. Наличие должностных лиц, ответственных за осуществление защиты информации, а также администраторов, осуществляющих практическую работу по обеспечению защиты информации, должно быть определено организационной структурой (штатным расписанием) УП «Брествторчермет» и должностными инструкциями.

5.7. Ответственность за обеспечение защиты информации должна быть возложена на каждого работника в пределах его полномочий.

5.8. Должны быть реализованы и поддерживаться следующие основные меры защиты информации в УП «Брествторчермет»:

правовые меры: соблюдение требований законодательства Республики Беларусь и ЛПА в УП «Брествторчермет» в области ИБ;

организационные меры: регламентация обеспечения особого режима допуска на территории (в помещениях), где может быть осуществлен доступ к информации (материальным носителям информации), регламентация разграничения доступа к информации по кругу лиц и характеру информации, а также определение технологических процедур администрирования;

технические меры: использование средств ТКЗИ, а также меры по контролю защищенности информации;

физические меры: воспрепятствование физическому проникновению посторонних лиц в помещения, в которых размещаются активы ИС и средства защиты информации.

6. Контроль соблюдения требований политики информационной безопасности. Порядок внесения изменений

6.1. Контроль соблюдения установленных в Политике ИБ требований по защите информации в процессе эксплуатации ИС осуществляет ответственный за ТКЗИ.

6.2. Для эффективного функционирования совокупности документированных правил, процедур и требований в области защиты информации, определенных в составе Политики ИБ, должны быть предусмотрены (после этапа разработки) этапы его внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения, включая определение и выполнение корректирующих и предупреждающих действий.

6.3. Ответственный за ТКЗИ систематически должен проводить анализ адекватности установленных политик и процедур действующим информационным процессам ИС, законодательству, возможностям вычислительных ресурсов, реальным угрозам ИБ.

6.4. Политика ИБ внепланово пересматривается при выявлении нарушения требований по защите информации, а также при изменении структуры, условий функционирования ИС, ИС и (или) сетей либо других факторов, влияющих на их актуальность.

6.5. Основаниями для внепланового пересмотра Политики ИБ также являются:

изменения законодательства Республики Беларусь в области информации, информатизации и защите информации;

решения руководства УП «Брествторчермет»;

инциденты ИБ, повлекшие значительный ущерб.

6.6. При пересмотре Политики ИБ должно учитываться следующее:

результаты независимого аудита ИБ УП «Брествторчермет»;

предложения работников и организаций-партнеров по совершенствованию защиты информации (ИБ) УП «Брествторчермет»;

результаты ранее проводившихся пересмотров Политики ИБ УП «Брествторчермет»;

изменения условий ведения бизнеса, законодательства, организационной структуры или ИС;

существующие угрозы и уязвимости ИС;

отчеты об инцидентах в области защиты информации (ИБ);

рекомендации Оперативно-аналитического центра при Президенте Республики Беларусь.

6.7. Результаты пересмотра Политики ИБ должны содержать решения по:

совершенствованию подхода к СЗИ в УП «Брествторчермет»;

уточнению целей и требований защиты информации (ИБ);

повышению эффективности СЗИ и уточнению сфер ответственности работников за обеспечение защиты информации (ИБ).

Инициаторами актуализации Политики ИБ могут выступать все субъекты информационных отношений по обеспечению защиты информации ИС.