УТВЕРЖДЕНО
Приказ республиканского
унитарного предприятия
«Национальный центр
электронных услуг»
от 24.07.2026 № 114

ПОЛИТИКА
информационной безопасности республиканского унитарного предприятия «Национальный центр электронных услуг»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Обеспечение информационной безопасности (далее – ИБ) является неотъемлемой частью деятельности республиканского унитарного предприятия «Национальный центр электронных услуг» (далее – Предприятие), направленной на создание цифровой среды, обеспечивающей защиту законных прав субъектов информационных отношений.

2. Настоящая Политика информационной безопасности республиканского унитарного предприятия «Национальный центр электронных услуг» (далее – Политика) определяет систему взглядов Предприятия на стратегические цели и задачи в области информационной безопасности.

3. Политика является документом верхнего уровня в документации Предприятия в области информационной безопасности, а также методологической основой для формирования и проведения на Предприятии единой политики в области информационной безопасности.

4. Политика представляет собой систематизированное изложение целей и задач защиты информации, основных принципов правовых, организационных и технических аспектов обеспечения информационной безопасности на Предприятии.

5. Политика разработана согласно требованиям 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 20.02.2020 № 66.

6. Для целей Политики применяются термины и определения, установленные следующими нормативными правовыми актами Республики Беларусь:

Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации»;

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»;

Положение о технической и криптографической защите информации, утвержденное Указом Президента Республики Беларусь от 16.04.2013 № 196,

а также следующие термины и определения:

информационная безопасность – состояние защищенности информации от внешних и внутренних угроз, при котором обеспечены конфиденциальность, целостность, подлинность, доступность и сохранность информации;

ИТ-актив – любой аппаратный, программный, сетевой, сервисный компонент ИТ-инфраструктуры;

ИТ-инфраструктура – комплекс взаимосвязанных аппаратных, программных, сетевых и сервисных компонентов, обеспечивающих обработку информации;

обработка информации – любое действие или совокупность действий, совершаемые с информацией, включая сбор, систематизацию, хранение, изменение, использование, блокирование, передачу, удаление информации.

7. Политика должна быть доведена до сведения всех работающих по трудовым договорам (контрактам) работников Предприятия, лиц, работающих по гражданско-правовым договорам, заключенным с Предприятием (далее – работниками Предприятия).

8. Политика утверждается директором Предприятия, а в его отсутствие по уважительным причинам (отпуск, служебная командировка, временная нетрудоспособность и т.п.) – лицом, его заменяющим, и публикуется в свободном доступе на официальном сайте Предприятия https://nces.by.

ГЛАВА 2
ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

9. Информационная безопасность на Предприятии обеспечивается за счет реализации комплекса мер по защите информации.

10. Основными целями защиты информации на Предприятии являются:

обеспечение непрерывности оказания услуг Предприятия и укрепление доверия к ним;

обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

сохранение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

11. Для достижения поставленных целей защиты информации должны быть решены следующие задачи:

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

реализация мероприятий по технической и криптографической защите информации;

регламентация и нормативное обеспечение процессов защиты информации путем формирования актуальной базы организационно-распорядительной документации;

определение ответственности и обязанностей субъектов информационных отношений;

повышение уровня знаний и навыков работников Предприятия по вопросам защиты информации;

непрерывный контроль за выполнением мер по защите информации;

регулярный анализ эффективности применяемых мер защиты информации и их совершенствование;

соблюдение требований законодательства об информации, информатизации и защите информации.

ГЛАВА 3
ОБЪЕКТЫ ЗАЩИТЫ

12. Защите подлежит:

информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу, в целях недопущения несанкционированного доступа к ней и несанкционированного воздействия на нее, обеспечения целостности и подлинности информации;

общедоступная информация в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней.

13. Требования Политики распространяются на информацию, обрабатываемую на ИТ-активах Предприятия, а также на информацию, обрабатываемую Предприятием на ИТ-активах сторонних организаций в рамках бизнес-процессов Предприятия.

14. Требования Политики распространяются на информацию, обрабатываемую на ИТ-активах сторонних организаций, размещенных в ИТ-инфраструктуре Предприятия, в объеме и на условиях, определенных договорными обязательствами.

ГЛАВА 4
ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

15. Защита информации на Предприятии осуществляется в соответствии со следующими принципами:

принцип законности: должны соблюдаться требования законодательства в области защиты информации;

принцип минимизации полномочий: при доступе к информации и ИТ-активам Предприятия должны предоставляться минимально необходимые права доступа, требующиеся для выполнения должностных или договорных обязанностей;

принцип разделения функций: обязанности работников Предприятия должны быть четко разделены, но с обязательным дублированием сфер ответственности между работниками Предприятия;

принципом нормативной обоснованности: порядок обеспечения защиты информации, обязанности и ответственность работников Предприятия должны быть регламентированы;

принцип осведомленности: работники Предприятия (и, при необходимости, иные субъекты информационных отношений) должны быть осведомлены о предоставленных им правах, а также накладываемых на них обязанностях и ответственности;

принцип непрерывности защиты информации: обеспечение защиты информации на всех этапах ее жизненного цикла;

принцип непрерывности совершенствования и развития системы обеспечения информационной безопасности. Должен осуществляться регулярный анализ эффективности применяемых мер защиты информации, выявляться их слабые места. Механизмы защиты должны обновляться в зависимости от изменения характера угроз.

ГЛАВА 5
ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛИТИКИ

16. Директор Предприятия несет персональную ответственность за организацию работ по защите информации на Предприятии.

17. Положения Политики обязательны для выполнения всеми работниками Предприятия, а также применяются в отношениях с контрагентами Предприятия (потребителями, поставщиками, партнерами, консультантами, практикантами и т.д.) – в договорах с контрагентами, получающими доступ к ИТ-инфраструктуре Предприятия, должна быть оговорена обязанность контрагентов по соблюдению требований информационной безопасности Предприятия в части, касающейся.

18. Неисполнение или ненадлежащее исполнение работниками Предприятия, контрагентами и потребителями услуг Предприятия обязанностей по обеспечению информационной безопасности может повлечь лишение их доступа к ИТ-активам Предприятия, а также применение к таким лицам мер воздействия, степень которых определяется в соответствии с требованиями законодательства Республики Беларусь.

ГЛАВА 6
КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛИТИКИ

19. Общий контроль состояния информационной безопасности Предприятия осуществляется директором Предприятия, а в его отсутствие по уважительным причинам (отпуск, служебная командировка, временная нетрудоспособность и т.п.) – лицом, его заменяющим.

20. Текущий контроль соблюдения настоящей Политики осуществляет подразделение Предприятия, на которое возложено обеспечение защиты информации.

21. Руководители самостоятельных структурных подразделений Предприятия обеспечивают регулярный контроль за соблюдением требований Политики работниками, состоящими в штате таких подразделений.

ГЛАВА 7
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

22. Требования по обеспечению информационной безопасности должны быть конкретизированы локальными правовыми актами,

организационно-распорядительной документацией Предприятия согласно целям, задачам и принципам, изложенным в Политике.

23. Положения Политики подлежат анализу для определения их актуальности и необходимости внесения изменений и (или) дополнений ежегодно, а также внепланово в следующих случаях:

перераспределение ответственности в части обеспечения информационной безопасности;

изменения законодательства в части информации и защиты информации;

выявление недостатков в существующей системе обеспечения информационной безопасности Предприятия.